CYBERSECURITY TIPS
SDPD Crime Prevention
October 15, 2015

CONTENTS

CYBERSECURITY FOR CHILDREN

Because we as individuals and businesses rely on computers for nearly everything in our daily lives, we need to be aware of the risks of using them and take appropriate measures to minimize dangers. Among these dangers are viruses that erase or corrupt information in computers, viruses that infect computers and then propagate and infect other computers, hackers that break into computers and create mischief or steal information, employees who steal confidential business information, predators who attempt to meet and sexually exploit children, etc. This paper contains tips for protecting against malware, securing mobile devices, and using the Internet. It also contains a variety of specific tips for businesses and parents. Many of these tips also apply to text messaging. To learn more about preventing cyber crime visit the FBI website at **www.fbi.gov/about-us/investigate/cyber**.

PROTECTING AGAINST MALWARE

Protecting Computers

Malware, which is short for malicious software, is computer code that's designed to disrupt computer operations, monitor and control online activity, or steal personal information. It includes the following:

- ***Viruses*** are programs that replicate themselves by infecting other programs. They often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing personal information, corrupting data, displaying political or humorous messages, spamming their contacts, or logging their keystrokes.
- ***Worms*** are standalone programs that replicate themselves in order to spread to other computers. Often, they use a computer network for this, relying on security failures on the target computer to access it. Unlike a computer virus, a worm does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
- ***Trojans*** are non-self-replicating programs containing malicious code that, when executed, carry out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. Trojans often employ a form of social engineering, presenting themselves as useful or interesting in order to persuade victims to install them on their computers.
- ***Scareware*** is a type of malware that is designed to trick victims into purchasing and downloading useless and potentially dangerous software. It usually appears as a pop-up that resembles Windows system messages and says that a large number of problems have been found on your computer and prompts you to buy software to fix the problems.
- ***Ransomware*** is a type of malware that restricts access to the infected computer system and demands a ransom paid to its creators to have the restriction removed.
- ***Spyware*** is software that gathers information about you, your computer, and your use of the Internet without your knowledge. It may also send that information to another entity or assert control over your computer.
- ***Adware*** is software that displays unwanted advertisements.

The following measures can help protect your computer from these dangers:

- Use strong passwords. Avoid using easily remembered numbers or available information like mother's maiden name, date of birth, hometown, names of relatives, ZIP code, phone number, etc. Passwords should have more than eight characters, with at least one capital letter, one lowercase letter, one number, and one symbol. Use of non-dictionary words or easily-remembered phrases is recommended, e.g. Johnhave3dawgs! Hackers can run a program that goes through the entire dictionary very quickly and crack any password which can be found in it. They can also use grammar rules to crack long passwords, especially those with pronouns. So use bad grammar

and nouns. For maximum security you should use randomly generated characters. Except for passwords created for one-time use, you should use different ones for each account or secure place. You can test your passwords and get advice on creating strong ones at **www.microsoft.com/protect/yourself/password/checker.mspx**.

- Here's a simple way to generate passwords for an account. It rates "best" in the Microsoft test. Start with the initials of the account in uppercase letters, e.g., BOA for Bank of America, followed by your initials in lowercase letters in parentheses, a blank space, the year you were born, and the initials of the account in lowercase letters. When you renew the password for the first time you would add the number 1 after the account initials. The rest of the password would not change. If your initials are xyz and you were born in 1957 the fifth renewal of password would be BOA5(xyz) 1957boa5. The initial password for an account at Wells Fargo Bank would be WFB(xyz) 1957wfb. The core of the password, (xyz) 1957 is the same for all passwords.
- Keep your computer up to date with the latest operating systems, applications, anti-virus (anti-malware) software and firewalls. The latter control incoming and outgoing network traffic based on an applied rule set. They establish a barrier between a trusted, secure internal network and the Internet or another network that is assumed not to be secure and trusted. Use security software that updates automatically. Visit **www.OnGuardOnline.gov** for more information. This also applies to multi-function printers, fax machines, and copiers that can be accessed using a web browser.
- Don't open any e-mail from an unknown sender. Delete it without opening it. "Drive-by spam" can automatically download malware when an HTML e-mail is opened. You don't have to click on a link or open an attachment to get infected. Another way to prevent this kind of attack is to deactivate the display of HTML e-mails and display e-mails in pure-text format only.
- Use security software that updates automatically. Visit **www.OnGuardOnline.gov** for more information.
- Don't buy or download free anti-virus software in response to unexpected pop-ups or e-mails, especially ones that claim to have scanned your computer and detected malicious software.
- Make sure the pop-up blocker in the tools menu of your browser is turned on. This will prevent most pop-up ads. If you do get one, be careful in getting rid of it. Never click on any of its boxes. By clicking on No or Close you may actually be downloading malware onto your computer. And even clicking on the X in the upper right-hand corner can initiate a download instead of closing the advertisement. To be safe on a PC, hold down the Ctrl and Alt keys and hit Delete. Then in the Windows Security box click on Task Manger, and then click on End Task. This will clear your screen. Then run a full anti-virus scan.
- Don't respond in any way to a telephone or e-mail warning that your computer has a virus even if it appears to come from an anti-virus software provider like Microsoft, Norton, or McAfee. "Helpful hackers" use this ploy to get you to download their software to fix the virus or sell you computer monitoring or security services to give them remote access to your computer so they can steal your passwords, online accounts, and other personal information. If you already have anti-virus software on your computer you'll receive a security update or warning directly on your computer.
- Turn off your computer and cover your webcam when you are not using them. The webcam can be controlled remotely if your computer has been compromised. Hackers have done this, captured nude photos of female victims, and threatened to release them publicly unless the victim agrees to send nude photos or videos, or engaged in a Skype session. This crime has been called sextortion. In it the hacker typically threatens to harm the victim's reputation by disclosing nude images.
- Use the latest versions of Internet browsers, e.g., Microsoft Internet Explorer 8, which is designed to prevent phishing attacks. Use Explorer in the "protected mode," which restricts the installation of files without the user's consent, and set the "Internet zone security" to high. That disables some of Explorer's less-secure features. And set your operating system and browser software to automatically download and install security patches.
- Don't install files or programs from CDs or flash drives before checking them for viruses.
- Scan demo disks from vendors, shareware, or freeware sources for viruses.
- Avoid using electronic bulletin boards.
- Don't download files from unknown sources.
- Don't allow any website to install software on your computers.
- Scan downloaded files for viruses. Avoid downloading executable files.

NIST Recommendations for System Patches and Malware Avoidance

The National Institute of Standards and Technology (NIST) publishes a series of computer security guides to help computer system managers protect their systems from hackers and malware. Vulnerabilities in software and firmware are the easiest ways to attack a system, and the two publications approach the problem by providing new guidance for software patching and malware avoidance.

A common method of avoiding attacks is to patch the vulnerabilities as soon as possible after the software company develops a patch, i.e., a piece of repair software for the problem. Patch management is the process of identifying, acquiring, installing, and verifying patches for products and systems. NIST's *Guide to Enterprise Patch Management Technologies*, Special Publication 800-40, Revision 3, July 2013, is available online at **http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf**. It is designed for agencies that take advantage of automated patch management systems such as those based on NIST's Security Content Automation Protocol (SCAP).

The second security document provides guidance to protect computer systems from malware, which is the most common external threat to most systems and can cause widespread damage and disruption. NIST's *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, Special Publication 800-83, Revision 1, July 2013, is available online at **http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf**. It provides information on how to modernize an organization's malware incident prevention measures and suggests enhancements to an organization's existing incident response capability to handle modern malware. It reflects the growing use of social engineering and the harvesting of social networking information for targeting attacks.

Protecting Mobile Devices

Cybercriminals are also targeting mobile devices with malware that compromises these devices. The Internet Crime Complaint Center (IC3), which is partnership between the FBI and the National White Collar Crime Center, suggests the following safety tips to protect them.

- When purchasing a smartphone, know the features of the device, including its default settings. Turn off features that are not needed to minimize the attack surface of the device.
- If the phone's operating system has encryption available, use it to protect your personal data in the case of loss or theft.
- With the growth of the application market for mobile devices, look at the reviews of the developer/company who published the application.
- Review and understand the permissions you give when you download applications. Understand their privacy and access setting. Be cautious in downloading applications and be aware of what data they access as a condition of their use. Look for comments other users post before downloading an application.
- Passcode protect your device. This is the first layer of physical security to protect its contents. In conjunction with the passcode, enable the screen lock feature after a few minutes of inactivity.
- Obtain malware protection. Look for applications that specialize in antivirus or file integrity that helps protect your device from rogue applications and malware.
- Be aware of applications that can track your location. They can be used by a criminal to assist a stalker or a burglar.
- Be aware that using jailbreak or rooting to remove certain restrictions imposed by the device manufacturer or cell phone carrier, which allows you nearly unregulated control over what programs can be installed and how the device can be used, often exploits significant security vulnerabilities and increases the attack surface of the device. Any time a user, application, or service runs in "unrestricted" or "system" level within an operational system, any compromise can take full control of the device.
- Don't allow your device to connect to unknown wireless networks. These networks could be rogue access points that capture information passed between your device and a legitimate server.
- If you decide to sell your device or trade it in, make sure you wipe the device (reset it to factory default) to avoid leaving personal data on the device.
- Install all smartphone updates to run applications and firmware. If you neglect this you risk having your device hacked or compromised.

- Avoid clicking on or otherwise downloading software or links from unknown sources.
- Use the same security precautions on your mobile phone as you would on your computer when using the Internet.

Smartphones continue to grow in popularity and are now as powerful and functional as many computers. To reduce their risk to security threats, the Federal Communications Commission (FCC) has published the following ten security tips. They are defined in detail at **www.fcc.gov/sites/default/files/smartphone_master_document.pdf**.

1. Set Personal Identification Numbers (PINs) and passwords to prevent unauthorized access to your phone.
2. Don't modify your smartphone's security settings.
3. Back up and secure your data. These files can be stored on your computer or on removable storage card.
4. Only install apps from trusted sources. Before downloading one, conduct research to ensure it is legitimate.
5. Understand app permissions before accepting them. Check the privacy settings for each app before installing them.
6. Install security apps that enable remote location and wiping. These apps can also help you locate and recover your phone when lost.
7. Accept updates and patches to your smartphone's software. Keep your phone's operating system software up-to-date by enabling automatic updates or accepting updates when prompted from your service provider, operating system provider, device manufacturer, or application provider.
8. Be smart when using public Wi-Fi networks. Limit your use of public hotspots and instead use protected Wi-Fi from a network operator you trust.
9. Erase data off your old phone before you donate, resell, or recycle it.
10. Report a lost or stolen smartphone to the local law enforcement agency and then register it with your wireless provider.

Here are some tips for safe mobile banking:

- Use your wifeless network when possible, not a Wi-Fi hot spot.
- Use Wi-Fi networks you know are secure.
- Make sure no one is looking over your shoulder to see your passwords.
- Know how to verify that a text message is from your bank. Your bank should tell you how to do this. This will protect you from smishing, as discussed below under Internet Fraud and Other Crimes.
- Use your bank's app to connect, not a mobile web browser. The former should be equipped with the latest data-encryption technology.
- Log out when finished.
- Check your phone periodically for unfamiliar apps that could be malware.

The FCC has also designed a tool to help smartphone owners who aren't protected against mobile security threats. It can be seen at **www.fcc.gov/smartphone-security**. To use this tool choose your mobile operating system from the four listed and follow the ten steps above to secure your mobile device. More about the Smartphone security can be found at **www.fcc.gov/blog/fcc-and-public-private-partners-launch-smartphone-security-checker-help-consumers-protect-mobil**.

SECURING MOBILE DEVICES

Smartphones, tablets, and other mobile devices are now as powerful and functional as many computers. Therefore is necessary to protect them just like you protect your computer or laptop. The Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT) provides the following tips to safeguard your personal information:

- Lock your device when you're not using it. Even if you only step away for a few minutes, it's enough time for someone else to steal or destroy information in it.
- Disconnect your device from the Internet when you aren't using it. The likelihood that attackers or viruses scanning the network for available devices will target you becomes much higher if your device is always connected.

- Keep security software up to date. Update security patches so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. Install them.
- Consider creating separate user accounts. If multiple people are using the device, someone else may accidentally access, modify, or delete your information. If you have the option, create different user accounts for each user and set the access and privileges for each account.
- Establish guidelines for usage. If multiple people using your device, especially children, make sure they understand how to use the device safely. Setting boundaries and guidelines will help protect your data.
- Back up your data. Whether or not you take steps to protect yourself, there will always be a possibility that something will happen to destroy your data. Regularly backing it up reduces the stress and consequences that result from losing important information.

Wi-Fi Hacking and Hotspot Dangers

Use of Wi-Fi in coffee shops, libraries, airports, hotels, universities, and other public places pose major security risks. While convenient, they're often not secure. You're sharing the network with strangers, and some of them may be interested in your personal information. If the hotspot doesn't require a password, it's not secure. If it asks for a password through your browser simply to grant access, or it asks for a Wired Equivalent Privacy (WEP) password, it's best to treat it as unsecured. You can be more confident that a hotspot is secure only if it asks for the Wi-Fi Protected Access (WPA and WPA2) password. WPA2 is more secure. However, a flaw in a feature added to Wi-Fi called Wi-Fi Protected Setup (WPS) allows WPA and WPA2 security to be bypassed and broken by brute force in many situations.

Also, unsecure laptops and smartphones make it easy for a hacker to intercept information to and from the web, including passwords and credit- or debit-card numbers. They are also vulnerable to malware infections, and to having their contents stolen or destroyed. A hacked laptop or smartphone can also create a security risk for the user's workplace if it contains a password to the corporate network. Wi-Fi users should take the following steps to reduce these risks:

- Turn the Wi-Fi on your laptop, PDA, and smartphone off when you aren't using the network. Otherwise your Wi-Fi card will broadcast your Service Set Identifier (SSID) looking for all networks it was previously connected to. This enables hackers to figure out the key that unscrambles the network password.
- Use a known service instead of Free Public Wi-Fi or similar risky, unknown signals called ad hoc networks.
- Check the Wi-Fi security policies of your service provider and install the protections they offer to ensure it's a known network and not an "evil twin" hacker site pretending to be the legitimate one.
- Pay attention to warnings that a Secure Sockets Layer (SSL) certificate is not valid. Never accept an invalid certificate on a public wireless network. Log off and look for a trustworthy network. Look for the padlock indicating an SSL connection. Keep your firewall on. And keep your operating system updated.
- Find out if your company offers a Virtual Private Network (VPN) and learn how to use it. Encrypted VPN sessions offer the highest security for public wireless use. Use Hypertext Transfer Protocol Secure (HTTPS) when accessing a website or use a VPN to protect the transmission of sensitive information when using a wireless connection.
- Upgrade your Wi-Fi cards. The older WEP security is easily hacked. The new WPA and WPA2 are much more resistant to attack.
- Secure IEEE 802.11 wireless access points with a WPA2 and Advanced Encryption Standard (AES) encryption to protect sensitive communications.
- If your router has the WPS function, disable it. Methods have been published for doing this for some models. But on others, disabling the WPS in the user interface is not effective and the device remains vulnerable to attack.
- Learn to connect securely. Even the vulnerable WEP offers more privacy and protection than an unsecured public connection. It's not something the average hacker can crack. Look at your connection page for a name and description. A legitimate wireless network is simply called a "wireless network." It will display an icon of just one connected computer. So called ad hoc or peer-to-peer networks that are used by scammers to steal your personal information scammers are not legitimate. The will be called "computer-to-computer" networks and display an icon of several computers connected together. Never connect to this network. And be sure to set up your computer so it doesn't automatically connect to a network but allows you to choose a connection.

- Only log in or send personal information on secure website pages, i.e., ones that are encrypted. They will have **https://** or **shttp://** in the Uniform Resource Locator (URL) and a "lock icon" at the top or bottom of your browser window. You can click on this icon to display information about the website and help you verify that it's not a fake.
- Use a unique, strong password for each account.
- When you've finished using an account, log out. Don't stay signed in.
- Pay attention to warnings from your browser if you try to visit a fake website or download a malicious program.
- Remove all passwords and browsing history after using a shared computer.
- Disable file-sharing on your laptop.
- Don't send any sensitive personal or business information while in a hotspot unless you absolutely have to.
- Put a strong password on your wireless network.
- In shopping, it's fine to browse website when you're out but wait until you are at home to do any online business.
- Be aware of the existence of malware that enables a mobile device to be used as an open microphone with or without the owner's knowledge.

How to Prevent Theft of Your Device

The theft of wireless devices, particularly smartphones, is sharply on the rise across the country. The high resale value of these devices has made them a prime target for robbers. And the personal information contained on them is very attractive to identity thieves. Things you can take to protect yourself, your device and the data it contains, along with things to if your device is stolen or lost are listed below.

- Pay attention to your surroundings when using your device in public. Don't focus on your device and don't use it if someone might grab it and run. If it's not urgent that you use your device, wait until you're in a secure and private place to do so.
- Don't let anyone "borrow" your device. If a stranger wants to make a call, offer to make it for him or her.
- Never leave your device unattended in a public place. And don't leave it visible in an unattended vehicle. Lock it in the glove compartment when you park, or in the trunk before you park.
- Never leave your device out in the open where it is easy to steal, e.g., in your back pocket. Keep it where it's harder to reach, e.g., in an inside pocket of your jacket.
- If you carry your device in a purse, use one with a shoulder strap. Keep the strap over your shoulder, the flap next to your body, and your hand on the strap. Hang the purse diagonally across your body and secure the flap.
- Record the device's make, model number, serial number, and unique identification number, i.e., either the International Mobile Equipment Identifier (IMEI) or the Mobile Equipment Identifier (MEID) number. Keep them in a safe place. The police may need this information if the device is stolen or lost.
- Review your warranty or service agreement to find out what will happen if your device is stolen or lost. Consider buying insurance if the policy is not satisfactory.

How to Protect the Data on Your Device

- Establish a strong password to restrict access. This will help protect you from unwanted usage charges and misuse of your personal data if your device is stolen or lost.
- Install and maintain anti-theft software if your phone doesn't have a kill switch. Apps are available that will:
  - Locate the device from any computer.
  - Lock the device to restrict access.
  - Wipe sensitive data from the device, including contacts, text messages, photos, e-mails, browser histories, and user accounts such as Facebook and Twitter.
  - Make the device emit an alarm to help the police locate it.
- Display contact information such as an e-mail address or phone number on your lock screen so that the device can be returned to you if it is lost and found. But don't include sensitive personal information such as your home address.
- Be careful about storing personal information on your device. Social networking and other apps may allow unwanted access to it.

- Back it up on your personal computer or other back-up device.
- Keep a list of all apps you have on your smartphone.
- See the section below on data privacy and security when traveling on business with mobile devices.

What to Do If Your Device Is Stolen

- Report the theft to the police as soon as possible. Include the make and model, and serial and IMEI or MEID numbers. Some carriers require proof that the device was stolen. A police report will provide that documentation.
- If you aren't sure certain whether your device was stolen or simply misplaced, attempt to locate it by calling it or by using its anti-theft software's GPS locator. Even if you have only lost it, you should remotely lock it to be safe.
- If your device has anti-theft software, use it to lock the device, wipe sensitive information, and/or activate the alarm. Note that under California Business and Professions Code Sec. 22761 any smartphone manufactured on or after July 1, 2015, and sold in California after that date, shall include a technological solution, commonly referred to as a kill switch, at the time of sale, to be provided by the manufacturer or operating system provider, that, once initiated and successfully communicated to the smartphone, can render the essential features of the smartphone inoperable to an unauthorized user when the smartphone is not in the possession of an authorized user. The essential features are defined as ability to use the smartphone for voice communications, text messaging, and the ability to browse the Internet, including the ability to access and use mobile software applications. Use of a kill switch will make your phone useless to thieves.
- Report the theft or loss to your carrier. You will only be responsible for charges incurred prior to when your report. If you provide your carrier with the IMEI or MEID number, your carrier may be able to disable your device and block access to the information it carries. Request written confirmation from your carrier that you reported the device as missing and that the device was disabled.
- Notify financial companies you have accessed with your device. Put banks and credit card companies on alert regarding your stolen or lost device and cancel their cards to prevent fraudulent transactions on your accounts.
- Change your passwords for al e-mail, banking, and social networking accounts that you have accessed with your device.
- Call ecoATM at **(858) 255-4111** to ask if your device has been sold in one of its kiosks. You will need a police report for it to investigate the theft.

INTERNET FRAUD AND OTHER CRIMES

In 2012 the IC3 received nearly 290,000 consumer complaints on its website. About 40 percent of these complaints reported financial losses. The total adjusted loss from these was about $525 million. You may be at risk if you answer "yes" to any of the following questions:

- Do you visit websites by clicking on links within an e-mail?
- Do you reply to e-mails from persons or businesses you are not familiar with?
- Have you received packages to hold or ship to someone you met on the Internet?
- Have you been asked to cash checks and wire funds to someone you met on the Internet?
- Would you cash checks or money orders received through an Internet transaction without first confirming their legitimacy?
- Would you provide your personal banking information in response to an e-mail notification?

If you become a victim of Internet fraud or receive any suspicious e-mails you should file a complaint with the IC3 at **www.ic3.gov**. Its website also includes press releases on the latest scams and other Internet dangers, and tips to assist you avoiding a variety of Internet frauds. You should also contact your e-mail provider. Most keep track of scams. Send your provider the suspicious message header and complete text. For more information on Internet fraud visit **www.LooksTooGoodToBeTrue.com**.

The following material deals with several specific kinds on Internet fraud and other crimes: e-mail scams, online shopping frauds, phishing, spear phishing, smishing, vishing, whaling, social network dangers, fake websites, e-card dangers, and unsafe drugs from online pharmacies.

E-mail Scams

Cybercriminals use e-mail in many clever ways to try to take your money and identity, and disrupt your computer operation, gather sensitive information, or gain unauthorized access to your computer. To protect your assets and computer you should never reply, click on any links, or open any attachments of e-mails that offer great bargains or something that's not legal. If you want to click on a link, check the URL first by hovering over it, not clicking, to see if the destination name matches the URL exactly. If it doesn't, it's a scam designed to take you to a fake website. And if you don't recognize the sender, you should delete the e-mail without even opening it. Be especially suspicious about the following:

- Business opportunities to make money with little effort or cash outlay
- Offers to sell lists of e-mail addresses or software
- Any offer that asks for an immediate response
- Chain letters
- Work-at-home schemes
- Health and diet claims of scientific breakthroughs, miraculous cures, etc.
- Get-rich-quick schemes
- Free goods offered to fee-paying group members
- Investments promising high rates of return with no risk
- Kits to unscramble cable TV signals
- Guaranteed loans or credit on easy terms
- Credit repair schemes
- Vacation prize promotions
- Renew magazine or newspaper subscriptions
- Special offers that require a credit check and a small fee for verification expenses to be paid by a credit or debit card
- Notices of prize or lottery winnings that require you to pay a fee to cover expenses
- Offers to enroll you in a health insurance plan under the ACA, commonly called Obamacare
- Requests for personal or financial information

Regarding the latter, cybercriminals often pose as government agencies or financial institutions that you normally deal with. Remember that government agencies never send important things by e-mail and your financial institutions already have your personal information.

If you suspect something might be a scam, check it out on Hoaxslayer at **www.hoax-slayer.com**. This website is devoted to debunking e-mail hoaxes and exposing Internet scams. It is constantly increasing its compiled list of scams. Regarding chain letters, US-CERT recommends being especially cautious if the e-mail has any of the following characteristics:

- Suggests tragic consequences for not performing some action
- Promises money or gift certificates for performing some action
- Offers instructions or attachments claiming to protect you from a virus that is undetected by anti-virus software
- Claims it's not a hoax
- Includes multiple spelling or grammatical errors, or the logic is contradictory
- Urges you to forward the message

If an e-mail looks suspicious, it is always best to err on the side of caution and delete the message or mark it as junk mail. And as always, think before you act and be wary of any communication that asks you to act immediately, requests personal information, or just sounds too good to be true.

Online Shopping Frauds

If you use a credit card the federal Truth in Lending Act limits your liability to $50 for any unauthorized or fraudulent charges made before you report the billing error. To protect yourself you need to write to your credit card company within 60 days after the date of the statement with the error and tell it: (1) your name and account number, (2) that your bill contains an error and why it is wrong, and (3) the date and amount of the error. You need to pay all other charges but not the disputed amounts.

Don't use a bank debit card when shopping online, especially on an unfamiliar website. If something goes wrong your account can be emptied quickly without your knowledge. This can result in overdrafts, fees, and an inability to pay your bills. The federal Electronic Funds Transfer Act provides some liability protection in the event of any fraudulent charges resulting from the loss or theft of your card, or your card data. In the latter case you would not be liable for any fraud charges if you report them within 60 days after you receive your bank statement. But even then your bank is not obligated to restore your funds for at least two weeks while it investigates. But if you fail to report the fraud charges within 60 days of receiving your bank statement there is no limit on your liability. So if have to use a debit card, use one that is reloadable. Then you only risk the amount you put on the card if something goes wrong.

Consumers should be aware that if a deal looks too good to be true, it probably is. In one scam the victim located a car on the Auto Trader website and contacted the seller directly by e-mail. He was told that the car would be shipped to him for inspection and approval if he wired the money to a bank account where it would be held in escrow. He wired the money but the car never arrived. To prevent this kind of scam consumers need to be diligent in verifying all the parties involved in the purchase by phone calls, face-to-face meetings, etc. In a similar case the consumer asked to see the car before wiring any money. The scammer ended all contacts at that point.

Another example involved a Craigslist ad for a vacation apartment rental in New York City. The renter was told he had to act fast and wire the money or he'd lose out on this good deal. All three elements of a typical scam were present in this case: (1) act fast or lose the deal, (2) wire the money, and (3) a price that was too good to be true. Scammers also use Craigslist and other websites to advertise rentals in your area. They will make a duplicate of a legitimate ad but with a much lower price and a different contact number. They will ask for cash upfront without showing the property or ask you to fill out an application with your Social Security Number (SSN) or other personal information. These are signs of the scam.

Online scams also promise great deals on airline tickets, timeshare properties, and vacation packages. The biggest red flag is when payment is requested by a wire transfer. It's difficult to track these transfers and almost impossible to get a refund. Check out the company offering the deal before making a purchase. If it and the deal appear to be legitimate, pay by credit card and not by wire. Then if the deal turns out to be fraudulent, you can dispute the charges as indicated above.

Phishing

In this e-mail scam identity thieves fish for personal information by sending realistic-looking e-mails that ask recipients to go to a bogus website and to verify their credit card number, password, Personal Identification Number (PIN), or other account information. The magnitude of this scam can be seen in the July 2012 *Phishing Activity Trends Report for the 1st Quarter of 2012* in which the Anti-Phishing Working Group said it detected all-time monthly highs of 56,859 unique phishing websites; 30,237 unique phishing reports or campaigns, each sending hundreds of thousands or millions of e-mails to consumers; and 392 spoofed brands in February 2012.

Legitimate banks and financial institutions don't send e-mails asking you to verify your account information. They already have it. The following are examples of scammers posing as the IRS, FBI, Federal Deposit Insurance Corporation (FDIC), and the Centers for Disease Control and Prevention (CDC).

Each year during tax preparation time there is a surge in the number of frauds by criminals posing as IRS officials to obtain personal information for identity theft. The IRS never sends out unsolicited e-mails or asks for detailed personal or financial information. Neither does it say you are entitled to a refund and you can get it by clicking on a link to a website and sending your personal information. Any such e-mails are frauds. Some phone calls from

someone stating they are from the IRS may also be frauds. If you are suspicious, contact the IRS at **(800) 829-1040** to find out if it has a legitimate need to contact you. Go to the IRS website at **www.irs.gov** for information on the latest scams and instructions on how to protect yourself from suspicious e-mails or phishing schemes. Beware of any websites claiming to be from the IRS that end in .**com**, **.net**, **.org**, etc. The IRS also recommends forwarding the suspicious e-mail to it at **phishing@irs.gov**.

The growing popularity of tax preparation software has led to a rise in e-mail scams targeted at do-it-yourself taxpayers. The fraudulent e-mails claim to come from a software provider and might offer a software update or download. They may ask for personal financial information or other sensitive data and contain links to websites that could download malware. Legitimate software providers routinely send customers e-mails advising them of the status of their tax returns but never ask for sensitive personal data. Any software updates should be done on your provider's website or desktop product. Also, forward any suspicious e-mails to your software provider's security center.

Fraudulent e-mails have also been sent out by criminals posing as FBI agents and officials. They give the appearance of legitimacy by using the FBI seal, letterhead, and pictures of the FBI Director. They may also claim to come from the FBI's domestic or overseas offices. Like the IRS, the FBI does not send out e-mails soliciting personal or financial information. For more information on this kind of fraud go to the FBI website at **www.fbi.gov** and click on New E-Scams and Warnings under Be Crime Smart.

Another agency that has become aware of fraudulent e-mails in its name is the FDIC. These ask recipients to "visit the official FDIC website" by clicking on a hyperlink that directs them to a fake website that includes hyperlinks that open a "personal FDIC insurance file" to check on their deposit insurance coverage. Clicking on these links will download a file that contains malicious software to collect personal and confidential information.

In 2009 the CDC issued a health alert warning people not to respond to an e-mail referencing a CDC-sponsored state vaccination program for the H1N1 (Swine Flu) contagion that requires registration on "www.cdc.gov." People that click on this embedded link risk having a malicious code installed on their computer. Examples of this and other hoaxes and rumors can be seen at **www.cdc.gov/hoaxes_rumors.html**.

In April 2014 the San Diego Superior Court alerted the public about a new scam involving unsolicited e-mails claiming to be from the court. One person who had an issue before the court received an attachment with the e-mail. That person opened the attachment and soon discovered it contained a virus. The Court reiterated to the public that it does not communicate with people with issues before the court by unsolicited e-mail or telephone. It also does not communicate regarding "missed jury duty" or cases of which you are unaware. You should delete these e-mails or disregard these phone calls.

A scam that's rampant during the holiday season involves e-mails that ask you to confirm an online purchase order or a package shipment by clicking an included link or attachment. This is done to trick you into giving up control over their computers and identities.

Use the following tips to counter phishing:

- Don't open any e-mail from an unknown sender, especially if it offers something sensational, e.g., a video of Osama Bin Laden's death. Delete it without opening it. "Drive-by spam" can automatically download malware when an HTML e-mail is opened. You don't have to click on a link or open an attachment to get infected. Another way to prevent this kind of attack is to deactivate the display of HTML e-mails and display e-mails in pure-text format only.
- Don't open any unexpected e-mail attachments.
- Don't give out any passwords or personal information or click on any links no matter what the e-mail says, e.g., that you will be locked out of your account if you don't provide the information, or that you owe money.
- Don't click on links in e-mail messages purporting to come from your bank or any other institution or business that you have an account with. Retype the address into your browser. If you do click on a link and are prompted to log in with your password, don't do it. Close your browser and log into your account to make a payment or do whatever the message said.

- Don't click on any links in unsolicited e-mails you receive from companies you do business with, e.g., from FedEx regarding an "undeliverable" package.
- Don't click on any links in e-mail messages from a friend or person you know unless the message states why the link is being sent specifically to you and you recognize the Uniform Resource Locator (URL) of the link as one that the person might send you. Often someone hacks into an e-mail account and sends a message to everyone in the address book with a link to a fake or malicious website. You should delete such e-mails and send your friend an e-mail about it. Friends then usually send a message to everyone in their address books saying "I've been hacked. Don't click on any links."
- Don't double click on any Internet pop-up with a link to an offer or provide any personal information in response to a pop-up offer. And never enter personal information on a pop-up page.
- Use the latest versions of Internet browsers, e.g., Microsoft Internet Explorer 10, which is designed to help protect against socially-engineered malware. Use Explorer in the "protected mode," which restricts the installation of files without the user's consent, and set the "Internet zone security" to high. That disables some of Explorer's less-secure features. And set your operating system and browser software to automatically download and install security patches.
- Make sure the website page you are entering sensitive information on is secure. You can tell it is secure when the address on the top of your screen where the Uniform Resource Locator (URL) is displayed begins with **https://** rather than **http://.** You can also look for a closed padlock or an unbroken key on the bottom of your screen to indicate the page is secure. If the lock is open the site or the key is broken, the page is not secure. Note that on many websites only the order page will be secure.
- Read the website's privacy policy. It should explain what personal information it collects, how the information is used, whether it is provided to third parties, and what security measures are used to protect the information. Consider taking your business elsewhere if you don't see, understand, or agree with the policy.
- Keep your computer up to date with the latest operating systems, applications, anti-virus software and firewalls. Use security software that updates automatically. Visit **www.OnGuardOnline.gov** for more information.
- Don't buy or download free anti-virus software in response to unexpected pop-ups or e-mails, especially ones that claim to have scanned your computer and detected viruses.
- Make sure the pop-up blocker in the tools menu of your browser is turned on. This will prevent most pop-up ads. If you do get one, be careful in getting rid of it. Never click on any of its boxes. By clicking on No or Close you may actually be downloading malware onto your computer. And even clicking on the X in the upper right-hand corner can initiate a download instead of closing the pop-up. To be safe on a PC, hold down the Ctrl and Alt keys and hit Delete. Then in the Windows Security box click on Task Manger, and then click on End Task. This will clear your screen. Then run a full computer security scan.
- Don't respond in any way to a telephone or e-mail warning that your computer has a virus even if it appears to come from an anti-virus software provider like Microsoft, Norton, or McAfee. "Helpful hackers" use this ploy to get you to download their software to fix the virus or sell you computer monitoring or security services to give them remote access to your computer so they can steal your passwords, online accounts, and other personal information. If you already have anti-virus software on your computer you'll receive a security update or warning directly on your computer.
- Look for valid trust marks to increase your confidence in using a website. Reputation trust marks like BBBOnline offer a basic level of proof that there is an actual business behind the website and that it follows proper business practices. Privacy trust marks like TRUSTe indicate that the business is aware of identity theft and personal data abuse and abides by the requirements of the trust mark provider in its privacy policy. A Secure Socket Layer (SSL) trust mark like VeriSign indicates that the site uses up-to-date encryption technology to scramble communications between the website and your computer. And security-scanning trust marks like McAfee SECURE indicate that the business uses a regularly scheduled security auditing service for its website to ensure that it is free of malware. Because a phisher could create a false trust mark and verification website, you cannot know that the mark is valid unless you click on it. A link will take you to the verification website of the trust mark provider. The trust mark is valid if its verification website has **https://** in its URL.
- Be careful in visiting websites that don't have trust marks.

Spear Phishing

This is a more sophisticated version of phishing. It targets groups of people who have something in common, e.g., they work for the same company, deal with the same financial institution, or attend the same college. The fraudulent

e-mails appear to come from organizations the potential victims would normally get e-mails from. Success in spear phishing depends on three things: (1) the apparent source of the e-mail must be a known and trusted individual or organization, (2) there is information in the e-mail that makes it look legitimate, and (3) the request for personal or company-privileged information, or direction to click on an included link must have a logical basis, e.g., to update usernames and passwords. The information needed for these things is obtained by hacking into the organization's computer network, data breaches, or combing through other websites, blogs, and social networking sites.

Spear-phishing attacks are often used by individuals conducting targeted, rather than opportunistic, attacks. Those responsible for the attack may be seeking precise information stored on an organization's network or systems rather than monetary gain. Every organization is at risk of being the target of a spear-phishing attack.

The success of these attacks depends on finding the weakest link in a corporate network. This is usually one person who falls for an authentic-looking e-mail. Thus, the company's employees need to be the first line of defense. Here are some things they should do to avoid becoming a spear-phishing victim and causing great harm to their company.

- Always treat unsolicited or unexpected e-mail containing attachments or links with caution, especially when the e-mail appears related to known events or projects.
- Remember that most companies, banks, agencies, etc. don't request personal information by e-mail. If in doubt, call the sender. But don't use the number in the e-mail. It's usually phony too.
- Use a browser with a phishing filter.
- Never open an attachment or follow a link from a suspicious e-mail to another website. Look up the URL and enter it manually.
- Never respond to a request to verify passwords.
- Become paranoid about e-mail.
- Report any suspicious e-mail to your company's Information Technology (IT) manager in accordance with its security policy. Also report this activity to the IC3 by filing a complaint at **www.ic3.gov**.

Spear phishing can best be mitigated at the company level with increased cybersecurity. When weighing available options for mitigation strategies, companies should begin by asking themselves what the current and future consequences would be if proprietary data, personally-identifiable information, research and development-related data, e-mail, or other critical information were stolen. The answers will define what the company should protect.

Companies should also try to protect their employees from receiving malicious e-mail. With access to all incoming e-mail and knowledge of the kinds of e-mail that each employee normally receives, a cybersecurity system could recognize unusual e-mail and warn employees of it, especially before significant events and meetings. It should also warn employees about social engineering and spear phishing related to these events and meetings. And it should measure expected network activity levels so that changes in patterns can be more easily identified.

Smishing

This is phishing with text messages instead of e-mails. "Smishing" is a term coined from Short Message Service (SMS) and phishing. In these scams you may receive a SMS stating that your account will be charged for some particular program or purchase unless you visit a given URL within two days to cancel the order. When you click on the cancel link you will download malware to your computer. Don't respond to these SMSs. Alternatively, the SMS may give you a phone number to call where you will be asked for personal information. Before calling verify that the number matches the number of the named institution, e.g., your bank. And never give out personal information unless you have initiated the call.

Vishing

In this scam criminals use Voice over Internet Protocol (VoIP) technology to make telephone calls from anywhere in the world pretending to be a legitimate business, often using a fraudulent called ID matching the identity of the misrepresented company. The term "vishing" comes from voice phishing. It directs recipients to call a telephone number where they are tricked into giving up personal financial information. They might receive an urgent recorded message telling them that their credit card has been compromised and directing them to call the following telephone

number immediately and punch in their 16-digit account number to verify their identity. Alternatively, you may receive an e-mail asking you to call a particular number to prevent your account from being blocked. Someone there will attempt to get you to give up personal information. The best defense against vishing is to treat any unsolicited telephone message with suspicion and only give your personal information out when you have initiated the call and are sure the other party is legitimate.

Whaling

In another scam known as "whaling" fake e-mails have been sent to high-ranking executives to trick them into clicking on a link that takes them to a website that downloads software that secretly records keystrokes and sends data to a remote computer over the Internet. This lets the criminal capture passwords and other personal or corporate information, and gain control of the executive's computer. In one case fake subpoenas have been sent to executives commanding them to appear before a grand jury in a civil case. The link that offers a copy of the entire subpoena downloads the malicious software.

Social Networking Dangers

Malware creators, identity thieves, burglars, and spammers are increasingly targeting users of social networking sites in an effort to steal personal data and account passwords. One of the tactics they use to gain access to this information involves sending social networking users e-mails that appear to come from online friends. For example, some Facebook users have been receiving e-mails from their "friends" that claim to contain a video of them. When they click on it they download malware that installs a malicious program on their hard drive. A virus known as Koobface sends itself to all the friends on the victim's Facebook profile. A new version of the virus also is affecting users of Myspace and other social networking sites. Cyber-criminals are tricking social networking users into downloading malicious software by creating fake profiles of friends, celebrities, and others. Security experts say that such attacks, which became widespread in 2008, are increasingly successful because more and more people are becoming comfortable with putting all kinds of personal information about themselves on social networking sites. They warn that users need to be very careful about what information they post because it can be used to steal their identities.

Facebook users should become a fan of its security page at **www.facebook.com/security**, which has posts related to all sorts of security issues, tips, resources, and other information. Of recent concern is Graph Search, a search feature started in January 2013. With it any user can type in your name and get personal information that you have not secured, your friends have seen and made public, and non-friends have generated or obtained from others.

Here are some common ways cyber scammers exploit social media connections. Others are listed on the page entitled *Internet Social Networking Risks* on the FBI website at **www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks**.

- Clickjacking. Hyperlinks are concealed under legitimate-looking clickable content. Clicking on what looks like a Facebook "like" or "share" button actually downloads malware that can allow direct access to your computer or mobile device.
- Quizzes. Most people like online quizzes. Cyber crooks like them too. After completing the quiz and entering in your personal information and cell number, you notice your cell phone bill has an unauthorized charge on it.
- Phishing requests. An e-mail lures you to a fake Facebook, LinkedIn, or Twitter page, where you enter your login. As a result, the cybercriminal now has your account information.
- Shortened URLs. Clicking on shortened links, which are often used on social media sites, can unknowingly direct you to a website that installs malware on your computer.
- Suspicious e-mails. These scams involve e-mails luring you to go to your social media account. Some examples of bait are free products or gift cards, celebrity gossip, free apps, extra storage for your e-mail account, or a security issue fix. Once you've clicked on the link you've exposed your computer or mobile device to malware.
- Following with ill intent. Burglars may use Twitter to follow your tweets. For example, if you announce you're not home, it's the perfect time for a burglar to know when to break in.

To avoid problems on social networks or anywhere in the Internet, users should:

- Choose your network carefully. Make sure you understand its privacy settings and find out if it monitors the content of postings.
- Be careful about installing extras. Many third-party applications let you do more with your personal page but criminals sometime use them to steal personal information.
- Read your network's privacy policy regularly to stay informed on how it uses or discloses your information. Choose to opt out of information sharing wherever possible.
- Customize your personal privacy settings so only your friends have access to the information you post. Default settings on many sites allow anyone to see information about you. Check your settings frequently because they could be compromised when the site is updated, e.g., when new features are added.
- Type the address of your site directly into your browser or put it in your list of favorites. Don't click on a link to your site on an e-mail message or another website because you might be entering account information into a fake site where your personal information could be stolen.
- Never post any information that you don't want made public. Even if it's available only to "friends" you have no control over what a "friend" does with it. You can't retract or delete it after it's copied from your site.
- Untag yourself from pictures and other information you share with friends.
- Remember all password questions you have used to log into another website or account in case you forget your password. Never post information that contains the answers. And remember information you have posted so you don't create password questions that a hacker can get the answers to.
- Never post any information that might make you or your property vulnerable, e.g., your address or travel plans, or attractive to a burglar, e.g., pictures of valuable artwork or electronics.
- Wait until you get home to post your vacation blog and photos. Remove geotags with a metadata removal tool if you publish photos on the Internet while you are away. Even better, turn off the geotagging feature on your smartphone.
- Don't click on any links, videos, programs, etc. provided in messages, even if a "friend" encourages you to click on them. Treat links in messages like those in e-mails.
- Get program updates from the company's website, not through a provided link.
- Scan your computer regularly with updated anti-virus programs.
- Know who your friends are and be careful about accepting and adding new ones. Be very cautious about revealing information about yourself if you chat with people you don't know. Identity thieves might create a false profile to get information from you.
- Avoid giving away your "friends" e-mail addresses and don't allow any social networking services to scan your e-mail address book.
- Be suspicious of anyone, even a "friend," who asks for money over the Internet.

Fake Websites

Cybercriminals are now creating fake websites that will receive high search-engine rankings and thus attract the attention of persons searching for information on a particular subject. Persons just visiting those sites risk having their computers infected with malware. And if they click on any links in those sites they risk becoming a victim of identity theft and various scams, e.g., ones that claim you can make a lot of money for a small initial investment. To avoid these problems users should:

- Keep your computer's anti-virus systems up to date with the latest firewalls and software.
- Use caution clicking on links that claim to provide videos or information on hot topics in the current news, e.g., the earthquakes in Haiti and Chile. And be aware that the bad guys are now tricking Google into telling you that the link is a PDF file, which makes it look more authentic.
- Don't click on links to other websites. Look up the address elsewhere and retype it into your browser.
- Check to see where you would actually go before you click on a link. You can do this by scrolling your mouse over the link and reading the address in the box that will pop up over the link. Don't click on the link if this address does not match the one in the link.
- Use the tips provided above to counter phishing.

Do the following to make sure a website is legitimate and not selling counterfeit goods, especially if you are planning to buy a name-brand product. Always remember that if the price seems too good to be true, it probably is.

- Don't ever buy an item that you learn about via spam.
- Check that the domain name is spelled correctly. Cyber criminals are known to engage in type- or cyber-squatting to lure unsuspected victims to fake websites where they try to obtain personal and financial information or install malware on the victim's computer. They would use a name Appple.com or Bestbuyh.com. The fake website would be designed to look like the real one. It might offer a discount coupon in exchange for personal information or a credit card number.
- Check that the domain name ends in **.com**, **.org**, or **.net**. Those ending in **.cn** for China or **.mn** for Mongolia are likely to be fakes.
- Check the logo and picture of the product, and the spelling and contact information on the website.
- Call the phone number posted and talk to a live person. Ask where the product can be seen and visit the store.
- Don't conduct business with an anonymous seller.
- Save copies of all e-mails and other documents involved in the transaction. Then if you discover that an item is counterfeit you have documentation to use in reporting the crime to the National Intellectual Property Rights Coordination Center (IPR Center) at **www.iprcenter.gov/referral**. It coordinates the activities of various U.S. government agencies in conducting investigations related to intellectual property.

During open enrollment for health insurance under the Affordable Care Act (ACA), commonly called Obamacare, scammers have created fake websites to make consumers think they are the official federal or state websites and thereby secure bank account routing numbers for automatic monthly payments and other personal identifying information for malicious use. The official federal website is **www.healthcare.gov**. The official one for California is **www.coveredca.com**. Go directly to these websites for information and plan enrollment. And do not click on any links to health insurance exchanges that you might get in an e-mail or find in an Internet search.

E-card Dangers

You receive an e-mail saying "A friend has sent you an e-card." The e-mail appears to be from a legitimate card company, but malware is downloaded into your computer when you click the link to see the card. You should delete the e-mail if you don't recognize the sender or if you are instructed to download an executable program to view the e–card. And make sure your computer has adequate anti-virus protection.

And even if you recognize the sender your computer could be harmed if the incoming e-mail is phony and you click on a link to an e-card or open an attachment. This happened around Christmas time in 2010 when employees of various government agencies received phony holiday messages that appeared to come from the White House.

Unsafe Drugs and Fraud by Online Pharmacies

Buying prescription drugs on the Internet is easy but finding a safe source is not. There are thousands of Internet drug outlets selling low-price prescription medications that may be counterfeit, contaminated, or otherwise unsafe. Many of these outlets are located outside the United States, don't require a valid prescription, offer foreign drugs or ones not approved by the U.S. Food and Drug Administration, have unsecure websites, don't provide a way to contact a licensed pharmacist by phone to answer questions, and don't comply with state and federal laws and/or the patient safety and pharmacy practice standards of the National Association of Boards of Pharmacy (NABP).

You can avoid the risks of dealing with these rogue websites, which constitute about 96 percent of those on the Internet, by using safe sources have been identified by the NABP in its Verified Internet Pharmacy Practice Sites (VIPPS) program. They are listed as Recommended Internet Pharmacies on its website at www.nabp.net. These sites have undergone and successfully completed the NABP's accreditation process that includes a review of all policies and procedures regarding the practice of pharmacy and dispensing of medicine over the Internet as well as an on-site inspection of facilities used by the site of receive, review, and dispense medicine. The NABP website also lists Not Recommended Internet pharmacies and sites that have received its e-Advertiser Approval. These sites offer only limited pharmacy services or other prescription drug-related services. They have also been found to be safe, reliable, and lawful.

Some online pharmacies only exist to obtain personal information and membership fees. Their e-mail ads offer a large variety of scheduled drugs without a prescription to members only. If you join you lose your membership fee and become vulnerable to identity theft.

Hacked E-mail

You might have been hacked if:

- People in your address book write that they are getting e-mails you didn't send. They might have seemingly random links or urgent pleas to wire money.
- Your sent-message folder has messages you didn't send, or it has been emptied.
- Your social media accounts have posts you didn't make.
- You can't log onto your e-mail or social media accounts.

Do the following if you've been hacked.

- Make sure you have security software and it's up to date. Install it if you don't have it. Only buy it from a reputable, well-known company.
- Run the software to scan your computer for viruses and malware. Delete any suspicious software and restart your computer.
- Set your security software, internet browser, and operating system to update automatically with the latest patches.
- Change your passwords. Make them strong so they will be hard to guess. If you use similar passwords for other accounts, change them too.
- Get advice your e-mail provider or social networking site about restoring your account. If your account has been taken over you might need to fill out forms to prove it's really you trying to get back into your account.
- Check your account settings. Make sure your signature and away messages don't contain unfamiliar links, and that messages aren't being forwarded to someone else's address. On your social networking service look for changes to the account since you last logged in, say a new "friend."
- Send an e-mail to people in your address book letting them know you've been hacked. Warn them about possible malicious links or fake pleas for money. Put their e-mail addresses in the Bcc: line to keep them confidential.

Do the following to prevent being hacked:

- Use strong, unique passwords for important sites, especially your financial accounts.
- Safeguard your usernames and passwords. Never provide them in response to an e-mail.
- Use multi-factor authentication if possible.
- Don't click on links or open attachments in e-mails unless you trust them. And don't forward random links.
- Download free software only from sites you know and trust.
- Don't treat public computers like your personal computer. And be careful any time you use public Wi-Fi.

SAFER USE OF THE INTERNET

Many U.S. Government agencies are involved in promoting safe cyber practices. The main ones are the DHS and the Federal Trade Commission (FTC). Four of their programs are described below.

National Cyber Awareness System

Persons with specific concerns about cybersecurity should visit the US-CERT's website at **www.us-cert.gov**. US-CERT leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. Its National Cyber Awareness System offers a variety of information for users with varied technical expertise. Those with more technical interest can read or subscribe to the Alerts, Current Activity Updates, or Bulletins. Those looking for more

general-interest pieces can read the Tips. Current Activity Updates provide timely information on security risks to help you better protect your systems from malware campaigns and mitigate new software vulnerabilities. It is updated frequently and typically contains less detail than Alerts, which warn about vulnerabilities, incidents, and other security issues that pose major risks. Bulletins provide weekly summaries of new vulnerabilities with patch information provided when available. Tips provide advice about common security issues for home and business users. They deal with general security, attacks and threats, e-mail and communication, mobile devices, privacy, safe browsing, software, and applications.

You can take the following to protect your privacy and personal information.

- Do business with credible companies. Before supplying any personal information online, consider the answers to the following questions: Do you trust the business? Is it an established organization with a credible reputation? Does the information on the site suggest that there is a concern for the privacy of user information? Is there legitimate contact information provided?
- Limit cookies to make sure that other sites are not collecting personal information about you without your knowledge. Choose to allow cookies only for the website you are visiting, and block or limit cookies from a third-party. Make sure that cookies are disabled if you are using a public computer.
- Don't use your primary e-mail address in online submissions. Submitting your email address could result in spam. Consider opening an additional e-mail account for use online if you don't want your primary e-mail account flooded with unwanted messages. Make sure to log onto the account on a regular basis in case the vendor sends information about changes to policies.
- Avoid submitting credit card information online. Some companies offer a phone number you can use to provide your credit card information. Although this does not guarantee that the information will not be compromised, it eliminates the possibility that attackers will be able to hijack it during the submission process.
- Take advantage of options to limit exposure of personal information. Default options on certain websites may be chosen for convenience, not for security. For example, avoid allowing a website to remember your password. If your password is stored, your profile and any account information you have provided on that site is readily available if an attacker gains access to your computer. Also evaluate your settings on websites used for social networking. The nature of those sites is to share information, but you can restrict access to certain information so that you limit who can see what.

Stop.Think.Connect

In 2009 President Obama recognized the need to increase education and dialogue about cybersecurity and issued the Cyberspace Policy Review, which became the blueprint for cybersecurity in the future. In this review the DHS was asked to create an ongoing cybersecurity awareness campaign. It was called Stop.Think.Connect and was launched in October 2010. It provides tips and resources for cybersecurity on its website at **www.dhs.gov/stopthinkconnect**. They include the following.

Before you use the Internet take time to understand the risks and learn how to spot potential problems.

- Stop hackers from accessing your accounts, set secure passwords.
- Stop posting and sharing too much, keep your personal information personal.
- Stop doing something if it doesn't feel right, trust your gut.
- Stop questionable online behavior, only do and say things online that you would do in real life.

Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact the safety of yourself and your family.

- Think about the information you want to share before you share it.
- Think how your online actions can affect your offline life.
- Think before you act, don't automatically click on links.
- Think about why you are sharing information online. Is it going to be safe?
- Think about why you're going to a website. Did you get it from someone you trust?
- Think **a**bout who you're talking to online. Do you *really* know who they are?

Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

- Connect over secure networks.
- Connect with people you know and trust.
- Connect with care and be on the lookout for potential threats.
- Connect safely and show your friends and family how to behave online.
- Connect with websites you trust.

The following tips come from **www.stopthinkconnect.org**.

Keep a clean machine:

- Have the latest security software, web browser, and operating system.
- Use programs that automatically connect and update your security software.
- Protect all devices that connect to the Internet from all malware.
- Set up local administrator accounts on your computing devices so only an administrator (you) can download programs and applications. Then only download from a trusted source. If you have any questions about the legitimacy of a site, don't download from it.
- Use your security software to scan all USBs and other external devices before attaching them to your computer.

Protect your personal information:

- Secure your accounts with unique, strong passwords that have more than eight characters with at least one capital letter, one lowercase letter, one number, and one symbol.
- Keep a list of your passwords stored in a safe place away from your computer.
- Use privacy and security settings to limit who you share information with.

Connect with care:

- Delete any suspicious e-mail, tweets, posts, and online advertising. When in doubt, throw it out.
- Limit the business you conduct from Wi-Fi hotspots and adjust your security settings to limit who can access your computer.
- Secure your home wireless network. The minimum level of encryption is WPA2. Replace your router if it can't run WPA2. Protect your router with a strong password. The following website has good information on wireless routers: **www.onguardonline.gov/articles/0013-securing-your-wireless-network**.
- Use only secure websites when banking and shopping, i.e., ones with **https://** or **shttp://** in their addresses.

Be web wise:

- Keep pace with new ways to stay safe online by checking trusted website for the latest information.
- Think before you act when you are implored to act immediately, offered something that sounds too good to be true, or asked for personal information.
- Back up your valuable information by making an electronic copy and storing it in a safe place.

Be a good online citizen:

- Practice good online safety habits.
- Post about others as you would have them post about you.
- Report all types of cybercrime to you local law enforcement agency and other appropriate authorities.

OnGuardOnline.gov

The FTC manages this website in partnership with the DHS in its Stop.Think.Connect campaign, and many other federal agencies. Its website, **www.OnGuardOnline.gov**, provides practical tips from the federal government to help you guard against internet fraud, avoid scams, secure your computers, protect your privacy, protect your kids online, be smart online, etc.

Stop.Think.Click

This effort defines seven practices for safer computing and provides tips on preventing identity theft, safe use of social networking sites, online shopping, Internet auctions, avoiding scams, and wireless security. It also provides a glossary of terms. The seven practices are:

1. Protecting your personal information
2. Knowing who you're dealing with
3. Using anti-virus software as well as a firewall
4. Setting up your operating system and web browser software properly, and updating them regularly
5. Protecting your passwords
6. Backing up your important files
7. Learning who to contact if something goes wrong online.

Go to **http://csrc.nist.gov/groups/SMA/fasp/documents/security_ate/stopthinkclick.pdf** for information from OnGuard Online about these practices and tips.

CYBERSECURITY FOR BUSINESSES

Cyber crimes involve the illegal use of or the unauthorized entry into a computer system to tamper, interfere, damage, or manipulate the system or information stored in it. Computers, including mobile devices, can be the subject of the crime, the tool of the crime, or the target of the crime.

As the subject of a crime, a criminal would use your computer or another computer to willfully alter the information stored in your computer, add fraudulent or inaccurate information, delete information, etc. Motives for this include revenge, protest, competitive advantage, and ransom.

As the tool of a crime, a criminal would use a computer to gain access to or alter information stored on another computer. In one common mode of attack a hacker would send a "spear phishing" e-mail to employees who have access to the business bank account. The e-mail would contain an infected file or a link to a malicious website. If an employee opens the attachment or goes to the website, malware or malicious software that gives the hacker access bank account log-ins and passwords would be installed on the computer. The hacker would then have electronic payments made to accounts from which the money would be withdrawn. Criminals also use computers to commit various frauds and steal identities and other information.

As the target of a crime, computers and information stored in them can be stolen, sabotaged, or destroyed. Trade secrets and sensitive business information stored in computers can be lost in these kinds of attacks.

If you answer "no" to any of the following questions you need to worry about your company's cybersecurity and you should take appropriate steps to get to "yes."

Do we know what's connected to our network?
Do we know what's running or trying to run on our networks?
Do we properly manage the people who have administrative permission to wander around our network?
Do we have an automatic system that continuously monitors our network?

Your computers and the information in them should be protected as any valuable business asset. The following tips deal with physical and operational protective measures, Wi-Fi hacking and hotspot dangers, personnel policies and employee training, malware protection, protecting your bank accounts, use of social media, preventing and dealing

with data breaches, and safer use of the Internet. For more details see National Institute of Standards and Technology (NIST) Interagency Report NISTIR 7621 entitled *Small Business Information Security: The Fundamentals*, dated October 2009. It and many other reports are available online under NIST IR Publications on **http://csrc.nist.gov**.

Also, consider joining the FBI's InfraGard, a partnership with the private sector with the goal of promoting an ongoing dialogue and timely communications between its members and the FBI. Its members gain access to information that enables them to protect their assets from cyber crimes and other threats by sharing information and intelligence. Go to **www.infragard.net** to apply for membership.

Physical Protective Measures

- Don't allow unauthorized persons to have access to any of your computers. This includes cleaning crews and computer repair persons.
- Install surface or cable locks to prevent computer equipment theft.
- Install computers on shelves that can be rolled into lockable furniture when employees leave their work areas.
- Locate the computer room and data storage library away from outside windows and walls to prevent damage from external events.
- Install strong doors and locks to the computer room to prevent equipment theft and tampering.
- Reinforce interior walls to prevent break-ins. Extend interior walls to the true ceiling.
- Restrict access to computer facilities to authorized personnel. Require personnel to wear distinct, color-coded security badges in the computer center. Allow access through a single entrance. Other doors should be alarmed and used only as emergency exits.

Special Measures for Laptops

Special security measures are needed for laptops to prevent them from being stolen and the data in them used to harm your business.

- Train employees in the need for special measures to protect laptops and their data wherever they may be used.
- Issue desktops instead of laptops to employees who seldom leave their offices.
- Have employees lock up their laptops when they are left unattended in their offices. Laptops should never be left unguarded.
- Have employees carry their laptops in a sports bag or briefcase instead of the manufacturer's bag.
- Don't leave a laptop visible inside vehicles or unattended in public places.
- If left unattended, secure the laptop with a cable lock to something that cannot be easily moved. Or install an alarm that will sound if the laptop is moved.
- Create a loss response team to monitor compliance with laptop and data security measures, investigate losses, assess data needs, and remove data no longer needed.

The following measures should be employed to protect your business in the event a laptop is lost or stolen.

- Have employees back up their files so they can be recovered if their laptop is lost or stolen. These back-up files should be kept in a separate, secure place.
- Protect data with strong passwords, i.e., ones that are at least eight characters in length and have at least one capital letter, one lowercase letter, one number, and one symbol.
- Don't store passwords on laptops.
- Determine if employees need all the data on their laptops to perform their jobs. Remove any data that is not needed.
- Encrypt all sensitive information so it cannot be compromised.
- Install software that will enable you to erase sensitive information when the thief logs onto the Internet.

The following measures can help you recover a laptop that has been lost or stolen.

- Keep a record of all laptop model and serial numbers so if one is recovered you can prove it is yours. Also keep the sales receipt and register the laptop with the manufacturer.
- Place stickers on the laptops with a phone number to call if one is lost and found by an honest person. But don't put the business name on it. That could be used by criminals to guess passwords or assess the sensitivity of the data stored on the laptop.
- Install hardware, software, or both to aid in recovery of the laptop. After you report the laptop lost or stolen the software enables a monitoring company to track the laptop when the thief logs onto the Internet. Hardware systems work the same but have a Global Positioning System (GPS) device that can pinpoint its location.
- Report the loss to the local law enforcement agency, and notify the manufacturer.
- Look for it on Craigslist and E-Bay.

Procedural and Operational Protective Measures

- Classify information into categories based on importance and confidentiality. Use labels such as "Confidential" and "Sensitive." Identify software, programs, and data files that need special access controls. Employee access should be limited to what he or she needs to do their jobs. No employee should have unlimited access, especially to personally identifiable information.
- Reevaluate the access needs of those in senior and supervisory positions as they are promoted.
- Clearly document and consistently enforce all policies and controls.
- Install software-access control mechanisms. Require a unique, verifiable form of identification, such as a user code, or secret password for each user. Install special access controls, such as a call-back procedure, if you allow access through a landline connection.
- Have your Information Technology (IT) manager change administrative password on a regular basis. A number of free tools are available for this if manual modification is not practical. This password should also be changed during non-business hours.
- If warranted, hire a dedicated **i**nformation security officer. It has been suggested that companies with this officer detect more security incidents and report lower financial losses per incident that those without one.
- Require that passwords be a random sequence of more than eight characters in length and have at least one capital letter, one lowercase letter, one number, and one symbol. Passwords should be changed at least every three months and not be shared. Employees should use a unique password for each system and service they use. This should be promoted for any online services employees use outside of company systems. There are many password management tools available that can help with this process.
- Employee user accounts should not have administrative privileges. This will prevent the installation of any unauthorized software or malicious code that an employee might activate.
- Change security passwords to block access by employees who change jobs, leave, or are fired. The latter become a high risk to your business for revenge or theft.
- Encrypt confidential data stored in computers and mobile devices, or transmitted by e-mail or over communication networks. Use NIST data encryption standards.
- Design audit trails into your computer applications. Log all access to computer resources with unique user identification. Separate the duties of systems programmers, application programmers, and computer programmers.
- Review automated audit information and control reports to determine if there have been repeated, unsuccessful attempts to log-on both from within and outside your facility. Look for unauthorized changes to programs and data files periodically.
- Use monitoring or forensic tools to track the behavior of employees suspected of malicious activities. Cyber crimes committed by malicious employees are among the most serious threats to networked systems and data. They can disrupt operations, corrupt data, exfiltrate sensitive information, or compromise an IT system. For more information on insider threats and how to prevent fraud see the *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector* published by the Carnegie Mellon University and Software Engineering Institute, July 2012. It can be downloaded at **www.sei.cmu.edu/reports/12sr004.pdf.**
- Pay closer attention to those in special positions of trust and authority, e.g. accountants and managers, because it is easier for them to commit high-value crimes.
- Monitor incoming Internet traffic for signs of security breaches.

- Make backup copies of important business information, i.e., documents, spreadsheets, databases, files, etc. from each computer used in your business. This is necessary because computers die, hard disks fail, employees make mistakes, malicious programs can destroy data, etc. Make backups automatically at least once a week if possible. Test the backups periodically to ensure that they can be read reliably. Make a full backup once a month and store it in a protected place away from your business.
- Delete all information stored in your printers, copiers, and fax machines at least once a week. Use a secure data deletion program that will electronically wipe your hard drives. Simply hitting the delete key will leave some data on the hard drive.
- Be careful in getting outside help with computer security problems. Call the San Diego District Office of the U.S. Small Business Administration at **(619) 727-4883** for advice and recommendations. Start with a list of vendors or consultants. Then define the problem, send out a request for quotes, examine each quote, and check the provider's references and history before hiring one.
- If you become a victim of Internet fraud or receive any suspicious e-mails you should file a complaint with the Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Crime Center NW3C, at **www.ic3.gov**. The IC3 website also includes tips to assist you avoiding a variety of Internet frauds.
- Beware of the Business E-mail Compromise (BEC) scam if your business works with foreign suppliers or regularly makes wire-transfer payments. In one version the e-mail account of a high-level executive is spoofed or hacked and a request for a wire transfer from the compromised account is made to a second employee in the company who is normally responsible for processing these requests. For more information on BEC scams see FBI Public Service Announcement, Alert No. I-012215-PSA dated Jan. 22, 2015 at **www.ic3.gov/media/2015/150122.aspx**. The IC3 suggests the following measures to help protect you and your business from becoming victims of a BEC scam.
  - Avoid free, web-based e-mail. Establish a company website domain and use it to establish company e-mail accounts.
  - Be careful what is posted to social media and company websites, especially job duties/descriptions, hierarchal information, and out of office details.
  - Be suspicious of requests for secrecy or pressure to take action quickly.
  - Consider additional IT and financial security procedures and Two-Factor Authentication (TFA), for example: verify significant transactions with telephone calls, use digital signatures, delete e-mail from unknown parties without opening it or attachments or clicking on links in it, and use Forward instead of Reply to respond to any business e-mails with the correct e-mail address typed in or selected from your e-mail address book to ensure the intended recipient's correct e-mail address is used.
  - Beware of sudden changes in business practices, e.g., if a current business contact suddenly asks to be contacted via their personal e-mail address when all previous official correspondence has been on a company e-mail.
  - Always verify via other channels that you use with a legitimate business partner.
- Develop a response plan to control the damage that can result from malicious insider activity. The response team would assist in investigating the fraud and use the lessons learned to prevent further fraud and improve the plan.
- Install a quality spam filter. The majority of cyberattacks and phishing attempts come through e-mail, and simply keeping spam out of your network can greatly reduce your risk.
- Protect your employees from receiving malicious e-mail. With access to all incoming e-mail and knowledge of the kinds of e-mail that each employee normally receives, a security system could recognize unusual e-mail and warn employees of it. It could also warn of e-mail that requests employees to open attachments, verify passwords, or go to another website.
- Adopt a "clean desktop policy," explain it to your employees, carry out periodic inspections, rectify any violations found, and cite employees for them. Keep a record of violations and provide additional training as necessary. The policy might require employees to do the following:
  - Log off computer when leaving it unattended.
  - Use a password-protected screensaver.
  - Memorize passwords or keep them locked up. Don't put them on sticky notes or pieces of paper on your desk.
  - Lock desks, filing cabinets, and office door at the end of the work day.
  - Lock up mobile devices, including laptops, tablets, smartphones, PDAs, CD/DVD discs, and USB drives, when not in use.

Personnel Policies and Employee Training

Employees, including contractors, can do a great deal of damage to a business by ignorance of security policies, negligence in protecting business secrets, deliberate acts of sabotage, embezzlement, and the public release of sensitive information. The following measures will help prevent this.

- Conduct a comprehensive background check on prospective employees. Check references, credit reports, schools attended, licenses, civil judgments, citizenship, criminal records, and personality traits. Checks can be contracted out to a Consumer Reporting Agency (CRA) or done in-house. In either case management should consult with legal counsel to ensure compliance with federal, state, and local laws. And with so many foreigners being employed, it is also necessary to comply with the laws governing a candidate's country of citizenship.
- Unless a business has sufficient in-house expertise and resources to do background checks, it should contract with a knowledgeable and reputable CRA that is familiar with and will comply with the federal Fair Credit Reporting Act (FCRA), California Investigative Consumer Reporting Agencies Act (UCRAA), Consumer Credit Reporting Agencies Act (CCRAA), and other laws enacted to protect consumers and job applicants. For checks on foreigners, look for a CRA with a presence in the candidate's country of citizenship. Here are some other tips to avoid legal liability:
  - Limit the number of job applicants you send to a CRA.
  - Don't rely on the agency's report alone.
  - Make sure you use the correct forms.
  - Keep all background check reports and other documents.
  - Give the CRA an "applicant" whose background is known so it's the thoroughness and accuracy of its report can be assessed. Also, independently verify some of the information provided.
  - Review each report carefully to determine if there's a job-related basis for disqualify an applicant.
  - Don't assume you can search public records and avoid liability.
  - Don't rush through the process or cut corners.
- A criminal record check should include arrests, convictions, and outstanding warrants. In considering this information in making employment decisions, follow the U.S. Equal Employment Opportunity Commission (EEOC) Enforcement Guidance No. 915.002 dated 4/25/2012 regarding the prohibition of discrimination under Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000e *et seq*. Best practices for employers include the following:
  - Eliminate policies or practices that exclude people from employment based on any criminal record.
  - Train managers and hiring officials in the EEOC Enforcement Guidance.
  - Develop a policy and narrowly-tailored procedures for screening applicants and employees for criminal conduct.
  - Identify essential job requirements and the actual circumstances under which the jobs are performed.
  - Determine the specific offenses that may demonstrate unfitness for performing such jobs.
  - Identify the criminal offenses based on all available evidence.
  - Determine the duration of exclusions for criminal conduct based on all available evidence.
  - Include procedures for individualized assessments.
- Test applicants for personality traits as well as job skills. Look for people who can work well with others, show compassion to and for others, respond well to criticism, and communicate frustrations effectively. Applicants that exhibit the following traits are worrisome:
  - An exaggerated view of their abilities, achievements, and potential value to an organization
  - Intolerant of criticism
  - Minimizes the significance of the work of others
  - Need for attention and approval
  - Excessively emotional
  - Overly moralistic
  - Strong beliefs on how things should be done
  - Unable to compromise, things are black or white and never gray, has the correct problem solution
  - Antisocial
  - Dishonest in background details and capabilities
  - Many job changes

  - Lawsuits with prior employers
  - Never had difficulties is past relationships
- Interview prospective employees. Seek to hire individual who are team-oriented, can respond well to criticism, and can deal well with conflicts, i.e., ones unlikely to become insider threats. Note that California employers are now prohibited from demanding usernames, passwords, and information related to social media accounts from job applicants and employees. The law also bans employers from firing or disciplining employees who refuse to divulge their social media information. This includes videos, photographs, blogs, podcasts, text messages, e-mail, online accounts, and website profiles. However, this prohibition does not apply to information used to access employer-issued electronic devices and is not intended to infringe on the existing rights and obligations of employers to investigate employee workplace misconduct or employee violations of other laws or regulations.
- Require vendors, suppliers, and other contractors to use similar standards in hiring their employees. Include language in all contracts that makes contractors liable for actions of their employees.
- Treat all employees fairly and make sure none are teased by their peers or supervisors because of their ethnicity, speech, financial situation, social skills, or other traits.
- Monitor activities of employees who handle sensitive or confidential data. Many computer crime schemes require regular, periodic manipulation to avoid detection. Watch for employees who work abnormally long hours, weekends, or holidays, refuse to take time off, or exhibit a sudden withdrawal in group activity. The latter represents dissatisfaction with the business, a common trait of people who are likely to engage in insider security breaches. Also watch for employees who collect material not necessary to their jobs, such as data printouts, software manuals, etc. Unreported foreign trips are also red flags. The biggest security threats come from employees, not foreign hackers.
- Conduct periodic background checks on existing employees and look for unexplained financial gains.
- Train your employees in your basic computer usage and security policies. Also cover penalties for not following your policies. And have employees sign a statement that they understand and will follow your policies.
- Train your employees about security concerns and procedures for handling e-mails, clicking on links to websites, responding to popup windows, and installing USB drives. For example, they should not open e-mail from an unknown sender, open unexpected e-mail attachments, click on any links in e-mail messages even if they look real, respond to popup windows, or install personal USB drives. As for USB drives, you should supply your employees with ones that have built-in encryption.
- Train your employees to be aware of what others, even their supervisors, are doing and to report any suspicious behavior that threatens your security.
- Conduct periodic re-training because people forget things. Use pamphlets, posters, newsletters, videos, etc.
- Prohibit your employees from using their work computers for online shopping. There is a chance that they might unwittingly land on a fake website with an address similar to that of a legitimate company, e.g., Appple.com instead of Apple.com. This would inadvertently expose your computer network to cyber attacks.
- Spread security training over time. Don't rely on one-time seminars by security professionals. Present information in small pieces.
- Make security messages visible. Use videos in training sessions. Put up posters at fax machines, shred bins, coffee rooms, and other places where employees gather. Change them at least once a month. Have a security column in the company newsletter.
- Know your employees. Get views from people in various departments. Be alert to key indicators that an employee may become an insider threat. These include the following:
  - Sudden, apparent devotion to work and working late and alone
  - Accessing data not needed or never used in the past
  - Asking about things they are not involved with
  - Excessive use of "I" in writings and speech
  - Frustration with position and failure to get promoted
  - Lifestyle well above salary level
  - Financial debt
  - Strong objections to procedural changes related to financial, inventory or supply matters
  - Drugs and alcohol abuse
  - Moonlighting with materials available at the business
  - Evidence of compulsive gambling, persistent borrowing or bad check writing

- Make employees aware of insider threats and encourage employees to observe and collect information that indicates stress, and report suspicious behavior. The goal should be to catch an employee in the early stages of stress so they can be helped and prevented from harming themselves or the business.
- Develop protocols that will prevent a departing employee from stealing anything or later harming the business. Remind the employee of the agreements regarding confidentiality, non-disclosure of business information or data, and non-competition that were signed on employment.

Malware Protection

Malware, which is short for malicious software, is computer code that's designed to disrupt computer operations, monitor and control online activity, or steal personal information. It includes the following:

- ***Viruses*** are programs that replicate themselves by infecting other programs. They often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing personal information, corrupting data, displaying political or humorous messages, spamming their contacts, or logging their keystrokes.
- ***Worms*** are standalone programs that replicate themselves in order to spread to other computers. Often, they use a computer network for this, relying on security failures on the target computer to access it. Unlike a computer virus, a worm does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
- ***Trojans*** are non-self-replicating programs containing malicious code that, when executed, carry out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. Trojans often employ a form of social engineering, presenting themselves as useful or interesting in order to persuade victims to install them on their computers.
- ***Scareware*** is a type of malware that is designed to trick victims into purchasing and downloading useless and potentially dangerous software. It usually appears as a pop-up that resembles Windows system messages and says that a large number of problems have been found on your computer and prompts you to buy software to fix the problems.
- ***Ransomware*** is a type of malware that restricts access to the infected computer system and demands a ransom paid to its creators to have the restriction removed.
- ***Spyware*** is software that gathers information about you, your computer, and your use of the Internet without your knowledge. It may also send that information to another entity or assert control over your computer.
- ***Adware*** is software that displays unwanted advertisements.

The following measures can help protect your computers from viruses, spyware, and other types of malware:

- Keep your computer up to date with the latest operating systems, applications, anti-virus (anti-malware) software and firewalls. The latter control incoming and outgoing network traffic based on an applied rule set. They establish a barrier between a trusted, secure internal network and the Internet or another network that is assumed not to be secure and trusted. Use security software that updates automatically. Visit **www.OnGuardOnline.gov** for more information. This also applies to multi-function printers, fax machines, and copiers that can be accessed using a web browser.
- Also install real-time e-mail and web security along with solutions that prevent data theft and loss of confidential information. Traditional anti-virus products don't provide this protection.
- Don't open any e-mail from an unknown sender. Delete it without opening it. "Drive-by spam" can automatically download malware when an HTML e-mail is opened. You don't have to click on a link or open an attachment to get infected. Another way to prevent this kind of attack is to deactivate the display of HTML e-mails and display e-mails in pure-text format only.
- Don't buy or download free anti-virus software in response to unexpected pop-ups or e-mails, especially ones that claim to have scanned your computer and detected malicious software.
- Make sure the pop-up blocker in the tools menu of your browser is turned on. This will prevent most pop-up ads. If you do get one, be careful in getting rid of it. Never click on any of its boxes. By clicking on No or Close you may actually be downloading malware onto your computer. And even clicking on the X in the upper right-hand corner can initiate a download instead of closing the advertisement. To be safe on a PC, hold down

the Ctrl and Alt keys and hit Delete. Then in the Windows Security box click on Task Manger, and then click on End Task. This will clear your screen. Then run a full anti-virus scan.

- Don't respond in any way to a telephone or e-mail warning that your computer has a virus even if it appears to come from an anti-virus software provider like Microsoft, Norton, or McAfee. "Helpful hackers" use this ploy to get you to download their software to fix the virus or sell you computer monitoring or security services to give them remote access to your computer so they can steal your passwords, online accounts, and other personal information. If you already have anti-virus software on your computer you'll receive a security update or warning directly on your computer.
- Use the latest versions of Internet browsers, e.g., Microsoft Internet Explorer 8, which is designed to prevent phishing attacks. Use Explorer in the "protected mode," which restricts the installation of files without the user's consent, and set the "Internet zone security" to high. That disables some of Explorer's less-secure features. And set your operating system and browser software to automatically download and install security patches.
- Don't install files or programs from CDs or flash drives before checking them for viruses.
- Scan demo disks from vendors, shareware, or freeware sources for viruses.
- Avoid use of electronic bulletin boards.
- Don't download files from unknown sources.
- Don't allow any website to install software on your computers.
- Scan downloaded files for viruses. Avoid downloading executable files.
- Obtain copies of your anti-virus software for your employees' home computers if they do some business work at home. Also ensure that your employees' home computers are protected by hardware and software firewalls between their system(s) and the Internet.

Protecting Bank Accounts

- Set up dual controls so that each transaction requires the approval of two people.
- Establish a daily limit on how much money can be transferred out of your account.
- Require all transfers be prescheduled by phone or confirmed by a phone call or text message.
- Require that all new payees be verified.
- Check bank balances and scheduled payments at the end of every workday rather than at the beginning of the day. Contact the bank immediately if anything is amiss. Timely action can halt the completion of a fraudulent transaction because transfers usually aren't made until the next morning.
- Inquire about your bank's defenses against cyberattacks and review the terms of your banking agreement with regard to responsibilities for fraud losses. Shop around for banks that provide better protections.
- Conduct online business only with a secure browser connection, which is usually indicated by a small lock in the lower right corner of your web browser window. Erase your browser cache, temporary Internet files, cookies, and history after all online sessions. This will prevent this information from being stolen if your system is compromised.
- If your bank does not offer TFA for your account, move it to another bank.

In November 2014 some cybersecurity researchers spotted a strain of malware designed to eavesdrop on company computers in order to steal personal information such as usernames and passwords. Its ultimate aim was to break into bank accounts and siphon off cash. The virus, called Dridex, is spread through infected e-mails sent by its developers to targets. The e-mails typically contain an infected Microsoft Office file and attempt to trick the user into opening the attachment. If the user opens the document, a macro embedded in it surreptitiously triggers a download of the Dridex banking malware, enabling it to first steal banking credentials and then attempt to generate fraudulent financial transactions.

In August 2015 the botnet that controlled much of the Dridex network was seized by the U.S. authorities and one of the co-conspirators arrested. The spread of the malware stopped immediately. However, the software itself still exists, and researchers warn that it be used by other criminal groups with their own botnets. The measures listed above along with those for protecting against most other malware attacks should protect a user's computers against a Dridex-type attack. Users should have an up-to-date antivirus program running on their computer that can intercept the infected attachments before they are seen. Users should also be careful of opening attachments sent from unrecognized e-mail addresses.

Using Social Media

While the use of social media can stimulate innovation, create brand recognition, generate revenue, and improve customer satisfaction, it has inherent risks that can negatively impact business security. Thus businesses need to develop a social media strategy and a plan to address the risks of business and employee use. These risks include the following:

- Data leakage or theft
- Data system downtime to clean malware
- Exposure of customer confidential information
- Spear phishing attacks on customers and employees
- Adverse legal actions
- Privacy violations
- Brand and reputation damage
- Loss of competitive advantage
- Infection of mobile devices
- Productivity loss from excessive employee use
- Circumvention of business controls

Some risk mitigation techniques for business and employee use of social media are listed below. For details on risks and mitigation techniques see the emerging technology white paper entitled *Social Media: Business Benefits and Security, Governance and Assurance Perspectives* published by the Information Systems Audit and Control Association (ISACA).

- Conduct awareness training to inform employees of the risks in using social media.
- Ensure that anti-virus controls are updated daily.
- Use content filtering to restrict or limit access to social media sites.
- Provide employees with clear guidelines regarding what information about the business can and cannot be posted on their personal sites.
- Limit use of social media on business computers and devices.
- Scan the Internet for unauthorized or fraudulent use of the business name or brand, or hire a brand-protection firm to do this.
- Require strong passwords for site access by its managers.
- Give customers periodic information updates to maintain awareness of potential fraud.
- Establish policies for the use of mobile devices to access social media.
- Install appropriate controls on mobile devices.
- Obtain access to employees' personal sites and monitor them for security breaches.

Cybersecurity Planning

The following resources are available to help businesses in cybersecurity planning.

FCC. One way small businesses can improve their cybersecurity is to use the Small Biz Cyber Planner that was created by the Federal Communications Commission (FCC) in collaboration with public and private sector partners, including the Department of Homeland Security, the National Cyber Security Alliance, and the Chamber of Commerce. It can be created and generated at **www.fcc.gov/cyberplanner**.

This planning guide, Small Biz Cyber Planner 2.0, is designed for businesses that lack the resources to hire a dedicated staff to protect themselves and their customers from cyber threats. Even a business with one computer or one credit card terminal can benefit from this tool. However, the FCC recommends that businesses using more sophisticated networks with dozens of computers also consult a cybersecurity expert on using the cyber planner. And the FCC provides no warranties with respect to the guidance provided by this tool and is not responsible for any harm that might occur from using it. The planner deals with the following topics.

- Privacy and Data Security. Nothing is more important than the security of your data. How you handle and protect it is central to the security of your business and the privacy expectations of all the people involved.
- Scams and Fraud. Telecommunication technology offers cyber criminals many ways to victimize your business, scam your customers, and hurt your reputation. You need to be aware of the most common online scams.
- Network Security. For this you need to: (1) identify all devices and connections on the network, (2) set boundaries between your systems and others, and (3) enforce controls to ensure that unauthorized access, misuse, or denial-of-service attacks can be thwarted or rapidly contained, and that your systems can recover from these threats.
- Website Security. Web servers that host the data and other content available to the public on the Internet are the most targeted components of a business' network. Cyber criminals are constantly looking for websites to attack. Thus it is essential that your servers and the network infrastructure that supports them be secure because a breach can cause loss of revenues and customer trust, and legal liability.
- E-mail. E-mail has become vital for everyday operations. It must be secure to ensure the privacy of its users and to protect customer and business information.
- Mobile Devices. Mobile devices such as smartphones, tablets and Wi-Fi enabled laptops, if not secure, can expose and compromise all your business networks.
- Employees. Businesses must establish formal recruitment and employment processes to control and preserve the quality of their employees. Otherwise they risk workplace violence, theft, embezzlement, lawsuits for discrimination in hiring, and other workplace problems.
- Facility Security. Protecting those who work in and visit your business should be one of your top priorities.
- Operational Security. These measures are designed to deny hackers access to any information about your operations and plans.
- Payment Cards. These measures prevent fraud, keep customer information safe, and enable you to meet obligations to your bank or payment services processor.
- Incident Response and Reporting. Even well-implemented security measures cannot prevent all breaches, so be sure to have procedures in place to respond to breaches if they occur.
- Policy Development and Management. All businesses should develop and maintain clear and robust policies for safeguarding critical business data and sensitive information, protecting their reputation, and discouraging inappropriate behavior by employees. These need to be tailored to your business and updated when needed to deal with new threats and problems.

U. S. Department of Health and Human Services. At **www.HealthIT.gov** under Providers and Professionals, Privacy and Security, and Security Risk Assessment (SRA) there is a SRA tool and video, a 10-step privacy and security plan, a *Guide to Privacy and Security of Health Information*, and other information for cybersecurity planning that can be used in any business.

Greater Houston Partnership. At **www.Houston.org/cybersecurity** you can fill out a Cybersecurity Self Assessment Tool to measure your vulnerability to a cyber attack. It will tell you whether you have good security measures in place, whether you should perform a risk-benefit analysis to determine what additional measures to install, and whether you need to invest in more cybersecurity. You should also review the guide entitled *Cybersecurity and Business Vitality*. Although it was prepared for Houston-area businesses, it is applicable anywhere for any business.

US-CERT. At **www.us-cert.gov/home-and-business** you can keep up to date on a variety of subjects related to cybersecurity. These include the basics of cloud computing, virus safety on social networking sites, understanding denial-of-service attacks, avoiding social engineering and phishing attacks, choosing and protecting passwords, 10 ways to improve the security of a new computer, etc. You can also get current activity, alerts, bulletins, and tips from the National Cyber Awareness System.

CERT Coordination Center. Before US-CERT, the Software Engineering Institute at Carnegie Mellon University ran the CERT Coordination Center. At **www.cert.org/information-for/managers** managers can use the material on this site, which includes podcasts, to keep their employees informed about cybercrime and help them protect your business from malicious attack. The site also provides answers to the following questions: Are your networks secure? Are you doing enough about insider threats? How resilient is your organization? How well are you incorporating

security into your products and services? Are you addressing the latest software vulnerabilities? Are you responding effectively to incidents? Do you know how a Computer Security Incident Response Team (CSIRT) can help you?

SANS Institute. At **www.SANS.org/security-resources** you can see the *Top 25 Software Errors* that lead to serious vulnerabilities, the *20 Critical Controls* for effective cyber defense, and 12 templates for various security policies from the SANS Security Policy Resource page. These include policies for computers, desktops, e-mail, Internet use, mobile devices, etc. There is also a short primer for developing policies.

NIST. Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the President issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, in February 2013. It directed NIST to work with stakeholders to develop a voluntary framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructure. NIST released the first version of the framework on February 12, 2014. It was created through collaboration between industry and government and consists of standards, guidelines, and practices to promote the protection of critical infrastructure. This framework and its companion roadmap can be used in any business. It is available on line at **www.nist.gov/cyberframework**.

U. S. Chamber of Commerce. The U.S. Chamber of Commerce has teamed with Bank of America, Microsoft, Splunk, and Visa up to provide businesses with the guide that gives small- and medium-size businesses tools for protecting computers and networks and responding to cyber incidents. The guide, *Internet Security Essentials for Business 2.0*, urges business owners, managers, and employees to adopt fundamental Internet security practices to reduce network weaknesses and make the price of successful hacking increasingly steep. It emphasizes the following points and can be downloaded at **www.uschamber.com/sites/default/files/legacy/issues/defense/files/020956_PDF_web.pdf**.

- All businesses should understand common online risks that may lead them to become victims of cybercrime.
- Perfect online security is unattainable, even for large businesses. But there are inexpensive practices that can be implemented to improve the security of your information, computers, and networks.
- Businesses need to know how and to whom to report cyber incidents and online crime.
- Cybersecurity is a team activity. Taking the actions recommended in this guide will have positive consequences for the security of businesses, communities, and the country. The interconnectedness of computers and networks in cyberspace means that the public and private sectors share responsibility.

Its website at **www.uschamber.com/issue-brief/internet-security-essentials-business-20** provides links to the guide mentioned above and the following Microsoft tools that businesses can use to teach employees how to protect company, customer, and employee information.

- Top Tips for Internet Security at Work, a printable, double-sided card
- Internet Security at Work PowerPoint, a 30-minute slide presentation with speaker's notes.
- Stay Sharp on Internet Safety at Work, information condensed into a 3-minute video.
- Test Your Internet Security IQ, a 10-question quiz to help spread awareness among your employees.
- Internet Security Begins With You, a poster to remind employees of their responsibilities for Internet security

Security for Mobile Devices

When it comes to security, most mobile devices are targets waiting to be attacked by cybercriminals. That's the conclusion of GAO-12-757, a September 2012 report to Congress by the U. S. Government Accountability Office. This report, entitled *Better implementation of Controls for Mobile Devices Should Be Encouraged*, can be downloaded from the GAO website at **www.gao.gov/assets/650/648519.pdf**. It lists a number of vulnerabilities and threats and suggests several security controls to combat them. These controls include the following:

- Enable user authentication. Configure devices to require passwords or PINs to gain access.
- Enable TFA for sensitive business information. It's usually done under Settings or Privacy. TFA makes if far more difficult for cybercriminals to break into online accounts.
- Verify to authenticity of downloaded applications.

- Install anti-virus software to protect against spyware and other types of malware.
- Install a firewall to protect against unauthorized connections by intercepting both incoming and outgoing connection attempts and blocking or permitting them based on a list of rules.
- Implement procedures to receive security software updates promptly.
- Install remotely disabling so that if the device is lost or stolen, it can be locked or its contents erased.
- Encrypt sensitive data.
- Install whitelisting software that permits only known safe applications to execute commands.
- Only install necessary applications.

Cybercriminals are also targeting mobile devices with malware that compromises these devices. The IC3 suggests the following safety tips to protect them.

- When purchasing a smartphone, know the features of the device, including its default settings. Turn off features that are not needed to minimize the attack surface of the device.
- If the phone's operating system has encryption available, use it to protect your personal data in the case of loss or theft.
- With the growth of the application market for mobile devices, look at the reviews of the developer/company who published the application.
- Review and understand the permissions you give when you download applications. Understand their privacy and access setting. Be cautious in downloading applications and be aware of what data they access as a condition of their use. Look for comments other users post before downloading an application.
- Passcode protect your device. This is the first layer of physical security to protect its contents. In conjunction with the passcode, enable the screen lock feature after a few minutes of inactivity.
- Obtain malware protection. Look for applications that specialize in antivirus or file integrity that helps protect your device from rogue applications and malware.
- Be aware of applications that can track your location. They can be used by a criminal to assist a stalker or a burglar.
- Be aware that using jailbreak or rooting to remove certain restrictions imposed by the device manufacturer or cell phone carrier, which allows you nearly unregulated control over what programs can be installed and how the device can be used, often exploits significant security vulnerabilities and increases the attack surface of the device. Any time a user, application, or service runs in "unrestricted" or "system" level within an operational system, any compromise can take full control of the device.
- Don't allow your device to connect to unknown wireless networks. These networks could be rogue access points that capture information passed between your device and a legitimate server.
- If you decide to sell your device or trade it in, make sure you wipe the device (reset it to factory default) to avoid leaving personal data on the device.
- Install all smartphone updates to run applications and firmware. If you neglect this you risk having your device hacked or compromised.
- Avoid clicking on or otherwise downloading software or links from unknown sources.
- Use the same security precautions on your mobile phone as you would on your computer when using the Internet.

Businesses should also develop a mobile-device security policy. The policy would define the rules, principles, and practices for employee use of mobile devices, whether they are issued by the business or owned by an employee. It should cover roles and responsibilities, infrastructure security, device security, and security and risk assessments. By establishing policies that address these areas, agencies can create a framework for applying practices, tools, and training to help support the security of wireless networks. The business should also train its employees in this policy to ensure that mobile devices are configured, operated, and used in a secure and appropriate manner.

Mobile device security is especially important when employees are allowed or even encouraged to use their own mobile devices, known as Bring Your Own Device (BYOD). Businesses need a policy for BYOD use so they can be sure that: (1) business and personal information are kept separate in the device, (2) malware on an employee's device doesn't get into the business network, (3) an outsider can't hack into the employee's device and get into the

business network or steal sensitive business information, and (4) all business data can be removed from the device when the employee leaves or if the device is lost or stolen.

Data Privacy and Security when Traveling with Mobile Devices

Corporate espionage is an increasingly serious threat for a business traveler. The perpetrator may be a competitor, opportunist, or foreign intelligence officer. In many countries, domestic corporations collect competitive intelligence with the help and support of their government. To mitigate this risk, critical business data should not be carried in print or on an electronic device unless it is absolutely necessary. If some must be carried, it should be encrypted. And the traveler should keep it on his or her person at all times. Mobile devices should never be unattended. Hotel safes are not adequate protection.

Security is also a concern when using business data in other countries. For example, the U.S. State Department's Bureau of Consulate Affairs advisory for the 2014 Sochi Olympics stated that "Travelers should be aware that Russian Federal law permits the monitoring, retention, and analysis of all data that traverses Russian communication networks, including Internet browsing, e-mail messages, telephone calls, and fax transmissions." Thus, conversations may not be private or secure, and wireless and other communications may be intercepted. Some measures that a traveler should take to protect business data before, during, and after travel are suggested below.

Before Travel:

- Minimize data taken on removable media such as CDs, DVDs, and thumb drives.
- Consider using a company-owned cell phone, laptop, and/or tablet that contains only necessary data to limit the loss of data if the device is lost, stolen, or confiscated.
- Back up all data taken and store it in a secure place while you are away.
- Clear your Internet browser's cache, cookies, history and temporary Internet files.
- Update data protection software prior to departure.
- Install full-disk encryption on laptops.
- Use the U.S. State Department website at **www.state.gov** for information on the country of travel and laws regarding bringing mobile devices in and out. For example, Russia has no restrictions on bringing laptop computers into the country for personal use. However, the software may be inspected upon departure. Hardware and software found to contain sensitive or encrypted data may be subject to confiscation. In some countries withholding passwords is a crime.
- Install new strong passwords on all devices, with different ones on each one.
- Configure settings to automatically wipe devices' data after a certain number of password entry failures.
- Check with your company's legal advisor and IT manager for other measures to take.

During Stay:

- Do not expect privacy in some countries. Phone calls, electronic transmission, and even hotel rooms may be monitored. Sensitive conversations, transactions, and data transfers should be kept to a minimum until you return.
- Be prepared to turn devices on and off, present all removable media to customs officials, and decrypt data for inspection at international borders.
- Keep social networking communications and business transactions separate on your devices.
- Consider buying local cell phones or local Subscriber Identity Module (SIM) cards. Prepaid local phones limit costs by not working after exceeding a maximum number of minutes. They are cheaper for local calls and have better connectivity. Buying local Pay As You Go (PAYG) SIM cards provide an added level of anonymity that may be good for privacy and security.
- Beware of Wi-Fi and hotspot dangers, as discussed in the next section.
- Do not loan your devices to anyone.
- Do not attach unknown thumb drives. They are notorious for computer infections.
- Report lost or stolen devices as soon as possible to all concerned parties, which might be your company, mobile service provider, etc. Also report the loss to local authorities.

On Return:

- Return company-owned borrowed devices.
- Test all devices and removable media for malware, unauthorized access, and other corruption. Do not connect them to a trusted network before testing.
- Reformat and rebuild any device found to be compromised. Then restore data from files backed up before your travel.
- Change passwords on all devices taken on travel.

Other safety and security measures for business travel outside the U. S. are contained in a FBI brochure at **www.fbi.gov/about-us/investigate/counterintelligence/business-brochure**.

Protecting Corporate Data in Hotspots

Your IT manager should also do the following to protect corporate data from hotspot dangers:

- Establish and enforce strong authentication policies for devices trying to access corporate networks.
- Require employees to use a corporate VPN and encryption when making connections and exchanging data. Better still, set up computers so that devices automatically connect to the VPN and encrypt data after making sure that the computer or device hasn't been lost or stolen.
- Make sure all devices and software applications are configured properly and have the latest patches.
- Ensure that corporate security policies prevent employees from transferring sensitive data to mobile devices or unauthorized computers.
- Provide employees with broadcast air cards that require a service plan so they don't have to use public hotspots for wireless connections.

Preventing and Dealing with Data Breaches

One hundred and sixty-seven data breaches affecting more than 500 California residents were reported to the State Attorney General's Office in 2013. This is a 28 percent increase over the number reported in 2012 when state law first required such reporting. To help California business deal with this growing problem the Attorney General published a paper entitled *Cybersecurity in the Golden State* in February 2014. It is available online at **https://oag.ca.gov/cybersecurity**. It suggests the following 10 measures to reduce the chances of becoming a victim of cybercrime: (1) Assume you're a target, (2) Lead by example, (3) Map and analyze your data, (4) Encrypt your data, (5) Bank securely, (6) Defend yourself, (7) Educate employees, (8) Be password wise, (9) Operate securely, and (10) Plan for the worst. It also provides basic guidance for preparing an effective cybersecurity incident response plan.

Another paper that provides information to help protect personal information in your business and prevent data breaches was published by the FTC in November 2011. It is entitled *Protecting Personal Information: A Guide for Business* and can be found online at **www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf**. It suggests the following five key principles: (1) Take stock, (2) Scale down, (3) Lock it, (4) Pitch it, and (5) Plan ahead. You should do the following for each.

1. Take stock: Know what personal information you have in your files and in your computers.

- Inventory all file-storage and electronic equipment. Know where your business stores sensitive data.
- Talk to your employees and outside service providers to determine who sends you personal information and how it is sent.
- Consider all the personal information you collect from customers, and how you collect it.
- Review where you keep the information you collect, and who has access to it.

2. Scale down: Keep only what you need for your business.

- Use Social Security Numbers (SSNs) only for required and lawful purposes. Don't use them for employee or customer identification.
- Keep customer credit or debit card information only if you have a business need for it. Don't keep any information you don't need.
- Change the default settings on your software that reads customer's credit or debit cards.
- Review the credit application forms and fill-in-the-blank web screens you use to collect data from potential customers, and eliminate requests for any you don't need.
- Use no more that the last five digits of credit or debit card numbers on electronically printed receipts that you give to your customers. And don't use the card's expiration date.
- Develop a policy for retaining written records that is consistent with your business needs and the law.

3. Lock it: Protect the information that you keep and transmit.

- Keep documents and other materials containing personal information in locked rooms or file cabinets.
- Remind employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- Create a security policy for your employees when using laptops in and out of your office. (See prior section on Special Measures for Laptops.)
- Control access to your building.
- Encrypt sensitive information you send over public networks or use a secure file transfer service. Don't send personal information by e-mail.
- Run up-to-date anti-virus programs on all your computers. Use a firewall to protect your computers and network. (See prior section on Malware Protection.)
- Require employees to use strong passwords.
- Set access controls so employees only have access to information they need for their jobs. (See prior section on Procedural and Operational Protective Measures.)

4. Pitch it: Properly dispose of what you no longer need.

- Create and implement secure information disposal practices for employees in your office and for those who travel or work at home.
- Train your staff to separate sensitive and other paper records. Dispose of the former by shredding, burning, or pulverizing them. Use cross-cut shredders. The latter can be put in the trash.
- Make shredders available throughout your office, especially next to the copiers.
- Remove and destroy the hard disk of any computer or copier headed for the junkyard. Or wipe them securely.
- Remove and securely wipe hard drives of rented copiers before returning them. Or clear the memory and change the pass codes.
- Destroy CDs, floppies, USB drives, and other data storage devices, or securely wipe them before disposal.
- Test how thoroughly factory resets and remote wipes destroy data on any smartphones your employees use in the business, and only permit them to use phones on which the data can be completely destroyed when the device is retired. If there is any doubt about this, use a hammer on the phone to make sure it does not get into the secondary market.

5. Plan ahead: Create a plan for dealing with security breaches.

- Organize a response team and designate a team leader to manage the activities.
- Draft contingency plans for dealing with various kinds of breaches, including hacking, lost laptop, etc.
- Investigate breaches immediately and take steps to eliminate existing vulnerabilities or threats to personal information.
- Disconnect a compromised computer from the Internet.
- Post information about the breach on your website and include the phone number and e-mail address of your customer service staff.

- Create a list of who to notify inside and outside of your business in the event of a breach. The latter include the appropriate law enforcement agencies, the persons whose information has been compromised, your customers and other businesses that may be affected, and the media.
- Draft notification letters and other written communications. Consult your attorney for state and federal notification requirements.
- Consider what outside assistance is needed, e.g., in forensics, media relations, etc.

Note that California Civil Code Sec. 1798.82 requires any person or business that conducts business in California and that owns or licenses computerized data that includes personal information to notify persons whose personal information has been compromised and specify the information involved. This notice requirement is triggered if the breach involves an individual's first name or first initial and last name in combination with one or more of the following data elements when either the name or the data elements are not encrypted: SSN; driver's license number or California identification card number; account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; medical information; health insurance information; or a user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account. The letter of notice should also recommend measures to take to deal with the breach, warn of attempts to obtain personal information by e-mail, and suggest that any such attempts be reported to your customer service staff immediately.

In addition to notifying persons whose personal information has been compromised, businesses should do the following to keep their customers informed about what they are doing to fix the problem and regain their trust.

- As with any crisis, the first thing your customers want to know is that you're aware of the situation and that you're on top of it. A simple statement that comes as soon as you are aware of the breach goes a long way towards muting initial panic. This initial response doesn't need to go into a lot of detail about how many were affected, what was hacked, and how it happened. Chances are you won't know that yet so a simple message that doesn't go beyond what you know is best.
- Make sure you have a spokesperson who can communicate effectively about the breach and what you are doing about it. That person does not always have to grant interviews to the press but can make statements on social media instead.
- Share verifiable facts quickly as they come in. Your goal is to get control of the situation and make yourself the most up-to-date source of accurate information. If you don't, others will put forth their own theories about the reason and extent of the attack.
- Keep the public and stakeholders in the loop as you move forward in your investigation using traditional, online, and even paid media. Your website should be THE best source for information. Show it there in three places: (1) the home page, (2) the number one item in your news section, and (3) on a dedicated page that deals with the breach.
- Offer your customers free credit monitoring as the first step to rebuilding their trust.
- Tell your customers what you're doing to protect them from breaches in the future.
- Make an apology that acknowledges the breach and demonstrates concern and compassion for its victims.
- After your IT staff has done its investigation and fixed the problems, assure your customers that cybersecurity is an ongoing concern and that you are working to prevent any breaches in the future.

In view of growing hacker activity and the high costs of dealing with data breaches, businesses should consider buying cyber insurance to cover expenses of complying with laws that require companies to notify customers and regulators when personal information has been compromised. The insurance would also cover expenses in dealing with computer viruses, and other cyber crimes. Businesses should also consider the following:

- Hire a computer security expert to evaluate your computers and website and suggest ways to protect them.
- Make sure your e-mail is secure by using a service provider that has proper security systems.
- Use another company to process credit card transactions. That company should guarantee that its systems are secure and use a service that helps to weed out fraudulent transactions.
- Encrypt names and data elements. Notice requirements are not triggered in this case.

Due Diligence when Buying or Merging with Another Company

Buying or merging with another company without analyzing how it protects its digital data could be as risky as buying a company without reviewing its financials. Cybersecurity should be an important part of the due-diligence process before acquisitions and mergers. The dangers of ignoring it have increased as data breaches become more common and many companies move their data offsite to a "cloud." Here are some questions that buyers should ask in its due diligence.

- What is your most sensitive data? Identify information such as trade secrets that hackers are most likely to target.
- Who is storing the data and where? Make sure that third parties who store the data have appropriate cybersecurity and cannot legally hold the data hostage in the event of a dispute.
- How is data protected from hackers? Cybersecurity experts should examine all aspects of the company's cybersecurity.
- How is data protected from internal leaks? Because rogue employees are the most likely source of data leaks, which employees have access to the data and what has the company done to prevent data leaks?
- Have there been past data breaches and how did the company handle them? What was done to prevent future breaches?

CYBERSECURITY FOR CHILDREN

While the Internet provides a way to stay connected with friends, it also exposes us and our children to increased risks of cyberbullying, cyber predators, identity theft, fraud, and phishing. In June 2012 the U. S. Department of Homeland Security's *Stop.Think.Connect Update* cited a study conducted by the National Cyber Security Alliance that found that children aged 8 to 18 spend an average of about eight hours a day online. If a child sleeps eight hours a night, one-half of the time he or she is awake is spent online. In order to protect yourself and your family from potential online dangers, it is important first to understand the risks. Did you know that?

- 20 percent of kids will have been a victim of cyberbullying by the time they graduate from high school according to the Cyberbullying Research Center.
- 79 percent of online teens agree that teens aren't careful enough when sharing personal information online according to a study by the Pew Internet and American Life Project.
- The Crimes against Children Research Center warns that one in five U.S. teenagers who regularly log on to the Internet say they have received an unwanted sexual solicitation via the web.
- 500,000 kid identities are stolen each year according to the Identity Theft Resource Center. In a MSNBC investigation officials found a 9-year-old girl in default on utility bills, a teenager $750,000 in debt, and a 2-year-old with a pile of credit card bills.

Although the vast majority of online services and Internet material is legitimate and benign, there have been numerous incidents of children receiving pornographic material, providing personal information under the pretext of possibly winning a prize, or sending money for promised benefits or products. Warning signs of these dangers include the following:

- Excessive late-night computer use
- Secretive behavior about computer associates
- Pornography
- Receiving phone calls, mail, gifts, or packages from persons you don't know
- Making phone calls to numbers you don't recognize
- Hidden files or directories, and password-protected bios, files, or logical drives
- Turning the computer monitor off or quickly changing the screen when you enter the room
- Becoming withdrawn from the family

If you are not familiar with computers, the Internet, and social networking you should visit **www.NetSmartz411.org**. It is parents' and guardians' premier online resource for answering questions about

Internet safety, computers, and the Web. There you can get answers to frequently asked questions. Or you can call **(888) 638-7411** to ask your questions to an expert. You can also visit the NetSmartz Workshop at **www.netsmartz.org**. It is an interactive, educational program of the National Center for Missing & Exploited Children (NCMEC) that provides age-appropriate resources to help teach children how to be safer on- and off- line.

The program is designed for parents, guardians, and children ages 5-17. It entertains while it educates with resources such as videos, games, activity cards, and presentations, and has the following goals:

- Educate children on how to recognize potential Internet risks
- Engage children and adults in a two-way conversation about on- and off-line risks
- Empower children to help prevent themselves from being exploited and to report victimization to a trusted adult

Minimizing Internet Dangers

You should do the following to minimize Internet dangers that your children may encounter:

- Start early. Talk to your children about online behavior, safety, and security as soon as they start using a computer, cell phone, or any mobile device. Have them show you the websites they visit, how they navigate through the Internet, and how they use social networking sites. To better understand the latter you should try networking yourself. This is a great way to connect with your children on computer-related matters.
- Help them find information online. Search together to find reliable source of information and learn to distinguish fact from fiction.
- Set reasonable guidelines and time limits for Internet and cell phone use, and social networking. Prohibiting Internet use is not a good idea because it is too easy for children to establish accounts at a friend's house or many other places. But do set time limits on computer use. People, not computers, should be their best friends and companions.
- Keep the computer in the family room or other area where its use can be monitored. Don't allow computers and mobile devices such as laptops and smart phones to be used in your children's bedrooms. And don't allow your children to have separate passwords and log-on names.
- Post clear, simple, easy-to-read rules for Internet use on or near the computer. Discuss these rules with your children and make sure they understand the reasons for them. Visit **www.NetSmartz.org** for examples of rules and safety tips. Your supervision and attention is the best way to protect your children when using the Internet.
- Know what Internet access your children have away from home, i.e., at a friend's home, libraries, schools, and cell phones and other wireless devices. Also have a plan to monitor their online activities there.
- Initiate conversations with your children about their Internet use. Communicate your values, be patient and persistent, and don't rush through conversations. Encourage your children to come to you with any problems they encounter online or anything that makes them uncomfortable.
- Your children are computer users and should have their own passwords and log-on names. Make sure they understand the importance of password and privacy protection, and not to share passwords or log-on names with anyone but you. Passwords should be more than eight characters in length and have at least one capital letter, one lowercase letter, one number, and one symbol. Use of non-dictionary words is also recommended. Easily remembered numbers or available information like mother's maiden name, date of birth, phone number, or pet's names should not be used.
- Have your children give you their passwords and log-on names, and share their blogs and online profiles with you. Be aware that they can have multiple accounts on multiple services. Search for you children's identifying information and monitor their screen name(s) and websites for inappropriate content.
- Have your children request your permission to exchange phone numbers or meet another child they have "talked" to online. Consider talking to the other child's parents about a meeting and accompanying your child to the meeting, which should be in a public place. Tell your children that caution is needed because people online are not necessarily who they might seem to be. Never allow them to meet someone they have "met" online without your permission.
- Discourage your children from visiting chat rooms, especially those with video, even if they claim to be child friendly. Persons who would harm children use these websites to entice children.
- Use filtering software to scan for offensive words and phrases in chat rooms and then end the conversations by signing off.

- Install a browser that limits the websites that your younger children can visit to those vetted by educational professionals. Some will send you periodic e-mails that detail you children's Internet activity.
- Install a monitoring service like McGruff SafeGuard. It's free for 30 days and also scans any chat or text conversations for bad language and other inappropriate communications. Go to **www.gomcgruff.com** for details of this service. Also look at the ESET Family Security Pack at **www.eset.com**.
- Have your children promise not to turn off any programs you might install to monitor their computer use.
- Understand how online services work.
- Supervise closely the choice of websites by young children. Monitor their online activities as they get older and more independent. Check the computer's cache and history to see what websites they have accessed. Also check their profiles and buddy lists.
- Learn the meaning of the acronyms your children use in texting. Go to **www.netlingo.com/acronyms.php** for a list of acronyms and their definitions, e.g., PAL means parents are listening.
- Make sure your child's screen name does not reveal any identifying information such as name, age, location, school. A screen name should be benign and innocuous, e.g., the first letter of each word in an easily-remembered phrase.
- Prohibit your children from downloading any games, movies, programs, etc., trying to win "free" things, or buying things online. You are the computer administrator and should be the only one who can install new software and programs.
- Tell your children it's not safe to put photos or any type of personally identifying information on a personal website without privacy settings, even if they promise to give the website address to people they know. Anyone in the world can access such a website. Also, personally identifying information should not be published on a group website or in an Internet yearbook. Group photos are preferable to individual photos only if no names are published.
- Children should be aware that file sharing programs for music and videos may be stealing copyrighted material and make their computers vulnerable to malware.

Dangers of Social Networking

Children who use social networking sites like Facebook and Myspace should be warned about online predators. These Internet offenders manipulate young people into illegal or inappropriate behavior by "grooming" them, i.e., building trust, appealing to their desire to be liked and understood, and playing on their natural curiosity about sex. All settings should be on "private." Visit social-networking websites with your children and show them what's OK and what's risky. Establish your own profile so you can monitor your children. Teach them to do the following to prevent and deal with any problems that might arise:

- Never to give out their name, address, phone number, photos, school, schedule, or any other personal information that can identify them. Avoid posting anything that would enable a stranger to find them, e.g., school names. Members' profiles become public information.
- Never say they are home alone.
- Don't post anything that they wouldn't want the world to know, especially anything or language that might embarrass them later, e.g., in applying for college or a job. What's uploaded can be downloaded and passed around by others and be posted online forever. It can't be taken back even if it's deleted from a site.
- Never send out any pictures of themselves, family members, or friends.
- Don't "friend" strangers. People aren't always who they say they are. Have your children ask permission before listing any adults as "friends," even if they are teachers, relatives, or your friends.
- Come to you to discuss any harassment, hate speech, and inappropriate content they receive.
- Check comments regularly. Ignore and don't respond to any that are mean or embarrassing. Just log off if the harassment bothers them.
- Avoid misleading people into thinking they are older or younger than they are.
- Don't talk about sex or use any sexually explicit language.
- Block people from sending messages or e-mail, or delete them from their "buddy list" if they harass you.
- Change their password if someone hacks into their profile. Change username and e-mail address if someone repeatedly bothers them.

- Have you contact the company that runs the site to have their profile deleted if it was created or altered without their knowledge.
- Talk to you if they are upset about what is being said about them. If they are scared or threatened you will contact a Juvenile Service Team officer at the nearest SDPD area station and inform their Internet Service Provider. Area station addresses and phone numbers are listed in the back of this paper.

Children also need to be given rules for using cell phones and be warned of dangers in their use. Rules should deal with when and where phones can be used, what they can and cannot be used for, and etiquette and safety in texting. You need to set good examples in the use of phones, e.g., not while driving. The following are some good rules for texting.

- Be polite and respect others. Avoid using shorthand that might lead to misunderstandings. Think about how a message might be read and understood before sending it.
- Ignore messages from people you don't know.
- Block numbers of people you don't want to hear from.
- Don't post your cell phone number on the Internet.
- Never provide personal or financial information in response to a text message.
- Use Cc: and Reply all: with care.
- Never engage in sexting, i.e., the sending or forwarding of sexually explicit photos, videos, or messages. In addition to risking their reputation, friendships, and employment and educational opportunities, they could be in violation of California Penal Code Secs. 288.2, 288.3, and 311 *et seq* if they create, forward, or even save this kind of message.

Once rules are set you need to remind your children about them and check to see that they are being followed. Here are some things to do:

- Discuss to consequences of breaking the rules.
- Review your child's "friends" list and delete any you don't know about.
- Review their text messages and block or set limits on text messaging and picture sending if you don't like what you see. Make sure they are not receiving any threatening or harassing messages, or are sending, receiving, or saving any sexts.
- Block unwanted callers.
- Check the browser history. If it's empty someone may be hiding something.

Cyberbullying

Cyberbullying is another problem you should talk to your children about. You should tell them that they can't hide behind the messages they send or pictures they post, and that hurtful messages not only threaten the victim, but they make the sender look bad and can bring scorn from peers. They should not make threats, spread lies, start rumors, distribute embarrassing pictures, or otherwise distribute or publish electronic messages of a harassing nature about another person with the intent to place that person in reasonable fear for his or her safety. Such messages are a misdemeanor under California Penal Code Sec. 653.2, and a person who sends them can be punished by up to one year in a county jail, by a fine of not more than $1,000, or both. Also, you should also make sure your own conduct does not encourage bullying, i.e., that you don't make mean-spirited comments about others or act unkindly to them.

You also need to be prepared to help your children if they become a victim of bullying. You should encourage them to show you any online messages or pictures that make them feel threatened or hurt. If you fear for your child's safety you should call the SDPD on its non-emergency number, **(619) 531-2000** or **(858) 484-3154**. Otherwise tell your child not to respond, save the messages and pictures for evidence, and keep you informed. Call the SDPD again if the bullying persists. Here are some other things your child should do:

- Report the bullying to the website or network where it appears.
- Delete the bully from your list of "friends" or "buddies," or block the bully's username or e-mail address.
- Share these measures with a friend who is a victim of bullying. Bullying usually stops quickly when peers intervene on behalf of the victim.

Reporting Attempted Sexual Exploitation

Any suspected online sexual exploitation or attempt by an adult to meet your child should be reported immediately to the San Diego Internet Crimes against Children Task Force at **(858) 715-7100** and the Cyber Tipline at **www.cybertipline.com** or **(800) 843-5678**. The former is the local law-enforcement agency that deals with these matters. The latter is managed by the NCMEC and is mandated by Congress to forward your information to the appropriate law enforcement agency for investigation. If your children or anyone in your home receives pornography depicting children or your children receive sexually explicit images, report the imagery to ICAC and keep it open on your computer until an investigator comes to see it. Don't copy or download it. In the meantime you can use your computer for other things or turn your monitor off.

Preventing Cyber Crimes

Children should also be warned about virus creators, identity thieves, and spammers. These cyber-criminals are increasingly targeting users of social networking sites in an effort to steal their personal data and the passwords to their accounts. One of the tactics they use to gain access to this information involves sending social networking users e-mails that appear to come from online "friends." For example, some Facebook users have been receiving e-mails from "friends" that claim to contain a video of them. When they click on it they download a virus that goes through their hard drives and installs malware. The virus, known as Koobface, then sends itself to all the "friends" on the victim's Facebook profile. A new version of the virus also is affecting users of Myspace and other social networking sites. Cyber-criminals are tricking social networking users into downloading malware by creating fake profiles of friends, celebrities, and others. Security experts say that such attacks, which became widespread in 2008, are increasingly successful because more and more people are becoming comfortable with putting all kinds of personal information about themselves on social networking sites. They warn that users need to be very careful about what information they post because it can be used to steal their identities.

To avoid these problems on social networking sites or anywhere in the Internet, you should warn your children to:

- Not to open any e-mail from an unknown sender. Delete it without opening it. "Drive-by spam" can automatically download malware when an HTML e-mail is opened. You don't have to click on a link or open an attachment to get infected.
- Not to click on any links, videos, programs, etc. provided in messages, even if a "friend" encourages you to click on them.
- Not to visit any sites that promise ways of bypassing parental controls or blocks set up by schools to prevent users from visiting sites such as Facebook. These sites are full of scams, malware, and offers for other services.
- Get program updates directly from the company's website, not through a provided link.
- Customize your personal privacy settings so only your "friends" have access to the information you post.
- Read your network's privacy policy regularly to stay informed on how it uses or discloses your information.
- Scan your computer regularly with an anti-virus program. Make sure the program is kept up to date, preferably automatically.
- Be suspicious of anyone, even a "friend," who asks for money over the Internet.
- Don't open or forward chain letters. Just delete them. They are nuisances at best and scams at worst. And many contain viruses and other types of malware.
- Watch out for "free" stuff. Don't download anything unless it's from a trusted source and it's been scanned with security software. "Free" stuff can hide malware.
- Don't buy or download free anti-virus software in response to unexpected pop-ups or e-mails, especially ones that claim to have scanned your computer and detected malicious software.
- Make sure the pop-up blocker in the tools menu of your browser is turned on. This will prevent most pop-up ads. If you do get one, be careful in getting rid of it. Never click on any of its boxes. By clicking on No or Close you may actually be downloading malware onto your computer. And even clicking on the X in the upper right-hand corner can initiate a download instead of closing the ad. To be safe on a PC, hold down the Ctrl and Alt keys and hit Delete. Then in the Windows Security box click on Task Manger, and then click on End Task. This will clear your screen. Then run a full anti-virus scan.

- Avoid all online games and quizzes that request personal information, including your e-mail address. Providing this information can put your identity at risk.

Additional Information

Additional information on Internet dangers to children and how to keep children safe online is available on numerous websites. These include the following:

- San Diego Internet Crimes Against Children Task Force at **www.sdicac.org**
- National Cyber Security Alliance at **www.staysafeonline.org**
- San Diego County District Attorney at **www.sdcda.org. S**ee the Protecting Children Online page under Protecting the Community.
- GetNetWise at **www.GetNetWise.org**
- FBI *A Parent's Guide to Internet Safety* at **www.fbi.gov/stats-services/publications/parent-guide/parent-guide**.
- NCMEC at **www.ncmec.org**. See resources for parents and guardians.
- NET CETERA: *Chatting with Kids about Being Online* at **www.onguardonline.gov**.
- *Living Life Online* at **www.ftc.gov/bcp/edu/microsites/livinglifeonline/index.shtm**.
- ConnectSafely at **www.connectsafely.org/** offers parent's guides, a collection of short, clearly written guidebooks that explain apps, services, and platforms popular with teens.
- Netsmartz Kids at **www.netsmartzkids.org/** provides interactive, educational, and age-appropriate resources to help teach children how to be safer online.
- Family Online Safety Institute at **www.fosi.org/good-digital-parenting/** gives advice, tips, and tools that empower parents to confidently navigate the online world with your kids.
- Savvy Cyber Kids at **www.savvycyberkids.org/default.aspx** offers curriculum that covers the concepts of security, privacy, bully response, and online ethics with engaging characters and in age appropriate language.
- Stop.Think.Connect Social Media Guide at **www.stcguide.com/explore/tips-trends** provides tips for parents and students on how to protect themselves on social media and includes many resources available to them. The Guide explains the cyber risks kids face when using social media and provides tips for talking to your kids about these risks.

Home Video Games

Children are spending increasing amounts of time playing video games, which include computer and console games. Games can have good and bad impacts. Children can learn useful information, skills, attitudes, and behaviors from them. They find them highly motivating by virtue of their interactive nature. But games can also have negative effects on children's health and behavior. The former include obesity, seizures, tendonitis, nerve compression, and carpal tunnel syndrome. The latter come primarily from violent games that lead to increased physiological arousal and aggressive thoughts, feelings, and behavior.

You can protect your children from these negative effects by limiting the time they play games, reading reviews and checking the ratings of games they might buy, and becoming familiar with the games by playing them with your children. You can get information and ratings of games on the websites of the Entertainment Software Rating Board and Common Sense Media at **www.esrb.com** and **www.commonsensemedia.org**, respectively.